AFS

Benutzerhandbuch

Version 3.6

GC12-2831-00

AFS

Benutzerhandbuch

Version 3.6

GC12-2831-00

Hinweis

Bevor Sie dieses Handbuch und das entsprechende Produkt verwenden, lesen Sie unbedingt die Basisinformationen unter „Bemerkungen” auf Seite 103.

Erste Ausgabe (April 2000)

Diese Ausgabe bezieht sich auf
- AFS for AIX, Version 3.6
- AFS for Digital Unix, Version 3.6
- AFS for HP-UX, Version 3.6
- AFS for Linux, Version 3.6
- AFS for SGI IRIX, Version 3.6
- AFS for Solaris, Version 3.6

und auf alle nachfolgenden Releases und Änderungen, bis in den neuen Ausgaben anderes angegeben wird.

Veröffentlichungen können Sie über Ihren IBM Ansprechpartner oder über die für Ihr Gebiet zuständige IBM Geschäftsstelle beziehen.

© Copyright International Business Machines Corporation 1989, 2000. Alle Rechte vorbehalten.

Inhaltsverzeichnis

Informationen zu diesem Handbuch . . . vii
Zielgruppe und Zweck vii
Dokumentenstruktur vii
So verwenden Sie dieses Dokument. . . . viii
Zugehörige Dokumente viii
Typografische Konventionen. ix

Kapitel 1. Eine Einführung zu AFS 1
AFS-Konzepte. 1
Client / Server-Betrieb 1
Verteilte Dateisysteme 1
AFS-Dateibereich und lokaler Dateibereich 2
Zellen und Standorte 2
Volumes und Mount-Punkte 3
Quoten von Volumes 4
Verwenden von Dateien in AFS 4
Der Cache Manager 4
Aktualisieren der Kopien von im Cache befindlichen Dateien 5
Wenn mehrere Benutzer Dateien verändern 5
AFS-Sicherheit 6
Kennwörter und gegenseitige Authentifizierung 6
Zugriffssteuerungslisten 7
Unterschiede zwischen UNIX und AFS . . . 8
Gemeinsamer Dateizugriff. 8
Anmelden und Authentifizierung 8
Zugriffsschutz für Dateien und Verzeichnisse 9
Maschinenausfälle 9
Ferne Befehle 10
Unterschiede in der Semantik von Standard-UNIX-Befehlen 10
Verwendung von AFS mit NFS. 11

Kapitel 2. Verwendung von AFS. 13
Anmelden und Authentifizieren bei AFS . . 13
Anmelden. 13
So melden Sie sich mit Hilfe eines für AFS modifizierten Anmeldedienstprogramms an 13
So melden Sie sich mit Hilfe einer aus zwei Schritten bestehenden Anmeldeprozedur an 14
Authentifizieren bei AFS 14
So authentifizieren Sie sich bei AFS . . . 16
So lassen Sie sich Ihre Token anzeigen . . 17
Beispiel: Authentifizieren in der lokalen Zelle 17
Beispiel: Authentifizieren als ein anderer Benutzer 18
Beispiel: Authentifizieren in einer fremden Zelle 18
Begrenzung von fehlgeschlagenen Authentifizierungsversuchen 18
So lassen Sie sich die Begrenzung fehlgeschlagener Authentifizierungsversuche und die Sperrzeit anzeigen. 19
Beenden einer AFS-Sitzung 19
So löschen Sie Token 20
Beispiel: Deauthentifizieren von einer speziellen Zelle 20
So melden Sie sich ab 20
Zugreifen auf den AFS-Dateibereich 21
AFS-Pfadnamen. 21
Beispiel: Anzeigen des Inhalts eines Verzeichnisses eines anderen Benutzers . . . 21
Zugreifen auf fremde Zellen 22
Ändern Ihres Kennworts. 22
So lassen Sie sich Ablaufdatum und Wiederverwendungsmaßnahme des Kennworts anzeigen 23
So ändern Sie Ihr AFS-Kennwort 24
So ändern Sie Ihr UNIX-Kennwort . . . 24

Kapitel 3. Anzeigen von Informationen zu AFS 25
Anzeigen der Quote eines Volumes 25
Anzeigen des Prozentsatzes der verwendeten Quote 26
Beispiel: Anzeigen des verwendeten Prozentsatzes der Quote 26
Anzeigen der Quote und weiterer Informationen zu einem Volume 26
Beispiel: Anzeigen der Quote und anderer Informationen zu einem Volume 27
Anzeigen der Quote und weiterer Informationen zu einem Volume und einer Partition 27

© Copyright IBM Corp. 1989, 2000

Beispiel: Anzeigen der Quote und weiterer Informationen zu einem Volume und einer Partition 27
Suchen von Dateien und Verzeichnissen. . . 28
Anzeigen der Position einer Datei oder eines Verzeichnisses 28
Beispiel: Anzeigen der Verzeichnisposition 28
Prüfen des Status von Server-Maschinen . . 29
Überprüfen des Status von Datei-Server-Maschinen 29
Beispiel: Überprüfen des Status von Server-Maschinen 30
Festlegen des Zugriffs auf fremde Zellen . . 30
Anzeigen fremder Zellen. 30
Anzeigen der Rangordnung von Servern . . 31
Anzeigen von Werten für die Server-Rangordnung 32

Kapitel 4. Zugriffsschutz für Verzeichnisse und Dateien. 33
Zugriffssteuerungslisten 33
Zugriffssteuerung auf Verzeichnisebene . . 34
AFS-ACL-Berechtigungen 34
Vier Berechtigungen für das Verzeichnis . 34
Drei Berechtigungen für die Datei. . . . 36
Acht zusätzliche Berechtigungen 36
Kurzformen für Mengen an Berechtigungen 36
Normale und negative Berechtigungen . . 37
Konfigurieren von DFS-ACLs 38
Verwenden von Systemverwaltungsgruppen in ACLs 38
Aktivieren des Zugriffs auf Unterverzeichnisse. 39
Erweitern des Zugriffs auf Serviceprozesse 39
Erweitern des Zugriffs auf Benutzer fremder Zellen. 40
Anzeigen einer ACL 40
Vorgehensweise beim Anzeigen einer ACL 40
Beispiel: Anzeigen der ACL in einem Verzeichnis 41
Beispiel: Anzeigen der ACLs in mehreren Verzeichnissen 42
Ändern einer ACL 42
Hinzufügen, Entfernen oder Editieren normaler ACL-Berechtigungen 43
Beispiel: Hinzufügen eines einzelnen ACL-Eintrags 44
Beispiel: Definition mehrerer ACL-Einträge in einem Verzeichnis 44
Hinzufügen, Entfernen oder Editieren negativer ACL-Berechtigungen 45
Beispiel: Definieren eines Eintrags im Abschnitt mit den negativen Berechtigungen 45
Beispiel: Wiederherstellen des Zugriffs durch Entfernen eines Eintrags aus dem Abschnitt mit den negativen Berechtigungen 46
Vollständiges Ersetzen einer ACL 46
Vollständiges Ersetzen einer ACL 47
Beispiel: Ersetzen einer ACL 47
Kopieren von ACLs von einem Verzeichnis in ein anderes 48
Kopieren einer ACL von einem Verzeichnis in ein anderes 49
Beispiel: Kopieren einer ACL von einem Verzeichnis in ein anderes 49
Verwendung der UNIX-Modusbits durch AFS 50
Beispiel: Inaktivieren des Schreibzugriffs für eine Datei 51

Kapitel 5. Verwendung von Gruppen . . . 53
Informationen zu Gruppen 53
Vorschläge zum effektiven Einsatz von Gruppen 53
Gruppennamen 54
Gruppenerstellungsquote 55
Anzeigen von Gruppeninformationen . . . 55
So lassen Sie sich die Gruppenzugehörigkeit anzeigen 56
Beispiel: Anzeigen der Mitglieder einer Gruppe 56
Beispiel: Anzeigen der Gruppen, zu denen ein Benutzer gehört 56
So lassen Sie sich die Gruppen anzeigen, die einem Benutzer oder einer Gruppe gehören 56
Beispiel: Anzeigen der Gruppen, die einer Gruppe gehören 57
Beispiel: Anzeigen der Gruppen, die einem Benutzer gehören 57
So lassen Sie sich einen Gruppeneintrag anzeigen 57
Beispiel: Auflisten von Informationen über eine Gruppe 58
Beispiel: Auflisten von Gruppeninformationen über einen Benutzer . . . 58
Erstellen von Gruppen und Hinzufügen von Mitgliedern 58

So erstellen Sie eine Gruppe 59
Beispiel: Erstellen einer Gruppe 60
So fügen Sie zu einer Gruppe Mitglieder hinzu 60
Beispiel: Hinzufügen von Mitglieder zu einer Gruppe. 61
Entfernen von Benutzern aus einer Gruppe und Löschen einer Gruppe 61
So entfernen Sie Mitglieder aus einer Gruppe 61
Beispiel: Entfernen von Gruppenmitgliedern 62
So löschen Sie eine Gruppe 62
Beispiel: Löschen einer Gruppe 62
So entfernen Sie veraltete ACL-Einträge. . 62
Beispiel: Entfernen eines veralteten ACL-Eintrags 62
Ändern des Eigners oder des Namens einer Gruppe 63
So ändern Sie den Eigner einer Gruppe . . 63
Beispiel: Ändern des Eigners einer Gruppe in einen anderen Benutzer 64
Beispiel: Ändern des Eigners einer Gruppe in die Gruppe selbst 64
Beispiel: Ändern des Eigners einer Gruppe in eine Gruppe 64
So ändern Sie den Namen einer Gruppe 64
Beispiel: Ändern des Suffixes *Gruppenname* einer Gruppe. 65
Beispiel: Ändern des Präfixes *Eignername* einer Gruppe. 65
Schützen von Gruppeninformationen . . . 65
Interpretieren der Zugriffscodemarkierungen 65
So stellen Sie die Zugriffscodemarkierungen einer Gruppe ein 66
Beispiel: Einstellen der Zugriffscodemarkierungen einer Gruppe 67

Kapitel 6. Fehlerbehebung 69
Fehler: Zugriff auf Datei kann nicht durchgeführt oder Datei kann nicht kopiert oder gespeichert werden 69
Problem: Eigener Eintrag wurde versehentlich aus einer ACL entfernt 72
Fehlernachricht: ″afs: Lost contact with fileserver″. 73
Fehlernachricht: ″*Command*: Connection timed out″. 73
Fehlernachricht: ″ fs: You don't have the required access rights on '*Datei*'″ 73
Fehlernachricht: ″afs: failed to store file″ . . 73

Anhang A. Verwenden des NFS/AFS Translator 75
Voraussetzungen für die Verwendung des NFS/AFS Translator 75
Zugriff auf AFS über den Translator 76
Authentifizieren auf einem unterstützten Betriebssystem 76
Authentifizieren auf einem nicht unterstützten Betriebssystem 76
Fehlerbehebung für den NFS/AFS Translator 78
NFS-Client-Maschine ist im Zustand ″Frozen″. 78
Warmstart des NFS/AFS Translator . . . 79
Systemfehlernachrichten 79

Anhang B. AFS-Befehlssyntax und Online-Hilfefunktion 81
AFS-Befehlssyntax 81
Beispiel für die Befehlssyntax 82
Regeln zur Verwendung von AFS-Befehlen. . 82
Leerzeichen und Zeilen 82
Abkürzungen und Aliasnamen für Operationscodes. 82
Weglassen von Argumentschaltern . . . 83
Abkürzungen für Schalter und Markierungen 83
Abkürzungen für Verzeichnisreferenzen. . 84
Häufig verwendete fs- und pts-Befehle . . . 84
Informationen zu den fs-Befehlen 84
Informationen zu den pts-Befehlen . . . 85
Anfordern von Hilfe in AFS. 86
Anzeigen von Befehlssyntax und Aliasnamen 86
Anzeigen von Beschreibungen des Operationscodes 87

Anhang C. Glossar 89

Index 97

Bemerkungen 103
Marken 106

Antwort. 107

Informationen zu diesem Handbuch

Dieser Abschnitt beschreibt den Zweck, den Aufbau und die Konventionen dieses Dokumentes.

Zielgruppe und Zweck

Dieses Handbuch beschreibt Konzepte und Verfahren für den Zugriff auf die im Dateibereich AFS enthaltenen Informationen. Es wendet sich an AFS-Benutzer, die mit UNIX, aber nicht unbedingt auch mit AFS vertraut sind.

Das erste Kapitel beschreibt grundlegende AFS-Konzepte und Richtlinien für seine Verwendung und faßt einige Unterschiede zwischen dem Dateisystem UNIX und AFS zusammen. Die verbleibenden Kapitel erklären, wie AFS-Basisfunktionen wie das Anmelden, das Ändern eines Kennworts, das Empfangen von Informationen, das Schützen von Dateien, das Erstellen von Gruppen und die Fehlerbehebung auszuführen sind. Für eine spezielle Aufgabe oder eine Gruppe zusammengehörender Aufgaben bedeutsame Konzepte werden im Zusammenhang und vor den Prozeduren dargestellt. Es werden viele Beispiele angeführt.

Anweisungen enthalten generell nur die Befehle und die Befehlsoptionen, die für eine spezielle Aufgabe erforderlich sind. Eine vollständige Liste der AFS-Befehle und eine Beschreibung aller zu den Befehlen verfügbaren Optionen finden Sie in *AFS Administration Reference*.

Dokumentenstruktur

Dieses Dokument besteht aus den folgenden Kapiteln.

„Kapitel 1. Eine Einführung zu AFS” auf Seite 1 stellt die grundlegenden Konzepte und Funktionen von AFS vor. Um AFS erfolgreich einsetzen zu können, ist es wichtig, mit den in diesem Kapitel beschriebenen Begriffen und Konzepten vertraut zu sein.

„Kapitel 2. Verwendung von AFS” auf Seite 13 beschreibt, wie die Basisfunktionen von AFS zu verwenden sind: Das Anmelden und das Authentifizieren, das Stornieren der Anmeldung, das Abmelden, der Zugriff auf AFS-Dateien und -Verzeichnisse und das Ändern Ihres Kennworts.

„Kapitel 3. Anzeigen von Informationen zu AFS” auf Seite 25 beschreibt, wie Informationen zur Quote des Volumes und zum Speicherort von AFS, zum

© Copyright IBM Corp. 1989, 2000

Status der Datei-Server-Machine und zu den fremden Zellen, auf die Sie zugreifen können, zur Anzeige gebracht werden können.

„Kapitel 4. Zugriffsschutz für Verzeichnisse und Dateien" auf Seite 33 beschreibt, wie Sie Ihre Daten mit Hilfe von AFS-ACls (ACL = Access Control List, Zugriffssteuerungsliste) schützen können.

„Kapitel 5. Verwendung von Gruppen" auf Seite 53 beschreibt, wie Gruppen zu erstellen und zu verwalten sind.

„Kapitel 6. Fehlerbehebung" auf Seite 69 entwirft Schritte, um spezielle Probleme zu diagnostizieren und zu korrigieren.

„Anhang A. Verwenden des NFS/AFS Translator" auf Seite 75 beschreibt wie das Umsetzungsprogramm NFS/AFS Translator zu verwenden ist, um von einem NFS-Client aus auf den Dateibereich von AFS zuzugreifen.

„Anhang B. AFS-Befehlssyntax und Online-Hilfefunktion" auf Seite 81 beschreibt die Befehlssyntax von AFS und wie Online-Informationen zu den Befehlen erlangt werden können.

„Anhang C. Glossar" auf Seite 89 definiert im *AFS Benutzerhandbuch* verwendete Terme.

So verwenden Sie dieses Dokument

Bevor Sie AFS verwenden, lesen Sie „Kapitel 1. Eine Einführung zu AFS" auf Seite 1. Halten Sie sich für Ihre ersten Schritte mit AFS als authentifizierter Benutzer an die in „Kapitel 2. Verwendung von AFS" auf Seite 13 beschriebenen Prozeduren. Dort wird beschrieben, wie auf Dateien im Dateibereich von AFS zuzugreifen und wie eine AFS-Sitzung zu beenden ist. Verwenden Sie je nach Bedarf die anderen Kapitel, um die dort beschriebenen Arbeitsgänge auszuführen.

Zugehörige Dokumente

Der Dokumentationssatz AFS Documentation Kit enthält weiterhin die folgenden Dokumente:

- *AFS Administration Reference* beschreibt detailliert die Syntax jedes AFS-Befehls und wendet sich an den erfahrenen AFS-Administrator, -Programmierer oder -Benutzer. Für jeden AFS-Befehl listet *AFS Administration Reference* Befehlssyntax, Aliasnamen und Abkürzungen, seine Beschreibung, Argumente, Warnungen und Ausgaben, Beispiele und zugehörige Abschnitte auf. Die Befehle werden in alphabetischer Reihenfolge behandelt.

- *AFS Administration Guide* beschreibt Konzepte und Prozeduren, die zum Verwalten einer AFS-Zelle notwendig sind, sowie in größerem Umfang die Abschnitte im *AFS Benutzerhandbuch*.
- *AFS Erste Schritte* liefert Anweisungen zum Installieren von AFS-Servern und -Cients.

Typografische Konventionen

In der vorliegenden Veröffentlichung werden folgende typografische Konventionen verwendet:

- Befehle und Optionen in Syntaxdefinitionen, Beispielen und Fließtext werden **fett** dargestellt. Namen von Verzeichnissen, Dateien, Maschinen, Partitionen, Volumes und Benutzern werden ebenfalls **fett** dargestellt.
- Variable Daten werden *kursiv* dargestellt. Dazu gehören die vom Benutzer angegebenen Informationen in Befehlszeilen und Teile der Eingabeaufforderung, die abhängig davon, wer den Befehl absetzt, verschieden sind. Neue Termini werden ebenfalls *kursiv* dargestellt.
- Beispiele für Bildschirmausgaben und Dateiinhalte werden in `Monospace-Schrift` dargestellt.

Zusätzlich dazu werden folgende Symbole in Befehlssyntaxdefinitionen verwendet. Dies gilt sowohl für die Dokumentation als auch für die Anweisungen der AFS-Online-Hilfefunktion. Geben Sie diese Symbole nicht beim Absetzen eines Befehls ein.

- Optionale Angaben werden in eckigen Klammern **[ ]** angegeben.
- Vom Benutzer angegebene Werte in AFS-Befehlen werden in spitzen Klammern < > angegeben.
- Ein hochgestelltes Pluszeichen + nach einem Argument bedeutet, daß das Argument mehrere Werte akzeptiert.
- Das Prozentzeichen % steht für die normale Befehls-Shell-Eingabeaufforderung. Einige Betriebssysteme verwenden möglicherweise ein anderes Zeichen für diese Eingabeaufforderung.
- Das Nummernzeichen # steht für die Befehls-Shell-Eingabeaufforderung für den lokalen Superuser **root**. Einige Betriebssysteme verwenden möglicherweise ein anderes Zeichen für diese Eingabeaufforderung.
- Das Pipe-Symbol | in einer Befehlssyntaxanweisung trennt Werte für ein Argument voneinander, die sich gegenseitig ausschließen.

Weitere Informationen zu AFS-Befehlen, einschließlich einer Beschreibung der Komponenten der Befehlsfolgen, erlaubter Abkürzungen und Aliasnamen, und darüber, wie die Online-Hilfefunktion zu den Befehlen einzusetzen ist, finden Sie in „Anhang B. AFS-Befehlssyntax und Online-Hilfefunktion” auf Seite 81.

Kapitel 1. Eine Einführung zu AFS

Dieses Kapitel stellt Grundkonzepte und Begriffe für AFS vor. Es setzt voraus, daß Sie bereits mit UNIX-Standardbefehlen, dem Dateizugriffsschutz und den Konventionen zu Pfadnamen vertraut sind.

AFS-Konzepte

AFS gestaltet für Benutzer die Zusammenarbeit mit denselben Dateien leicht, unabhängig davon, wo sich die Dateien befinden. AFS-Benutzer brauchen nicht zu wissen, auf welcher Maschine sich eine Datei befindet, und Administratoren können Dateien zwischen den Maschinen verschieben, ohne Benutzerzugriffe zu unterbrechen. Benutzer identifizieren eine Datei immer über denselben Pfadnamen, und AFS sucht automatisch die richtige Datei, wie es auch im lokalen Dateisystem einer einzelnen Maschine gehandhabt wird. AFS macht zwar den gemeinsamen Dateizugriff leicht, schadet aber der Sicherheit der gemeinsam benutzten Dateien nicht. Es realisiert ein hochentwickeltes Zugriffsschutzschema.

Client/Server-Betrieb

AFS verwendet ein Modell des *Client/Server-Betriebs*. Beim Client / Server-Betrieb gibt es zwei Typen von Maschinen. *Server-Maschinen* speichern Daten und führen Services für Client-Maschinen aus. *Client-Maschinen* realisieren die Verarbeitung für die Benutzer und greifen auf Daten und Services zu, die durch Server-Maschinen bereitgestellt werden. Einige Maschinen agieren sowohl als Clients als auch als Server. In den meisten Fällen arbeiten Sie auf einer Client-Maschine und greifen auf Daten zu, die sich auf einer Datei-Server-Maschine befinden.

Verteilte Dateisysteme

AFS ist ein *verteiltes Dateisystem*, das die Dateisysteme mehrerer Datei-Server-Maschinen vereinigt, und den Zugriff auf Dateien, die sich auf einer fernen Datei-Server-Maschine befinden, in derselben einfachen Weise ermöglicht wie auf Dateien auf der lokalen Platte. Ein verteiltes Dateisystem hat gegenüber einem herkömmlichen zentralisierten Dateisystem zwei wesentliche Vorteile:

- Gestiegene Verfügbarkeit: Eine Kopie einer allgemein zugänglichen Datei, wie die Binärdatei für ein Anwendungsprogramm, kann auf vielen Datei-Server-Maschinen abgelegt werden. Ein Ausfall einer einzelnen oder auch mehrerer Maschinen macht damit die Datei nicht notwendigerweise unzugänglich. Statt dessen werden Benutzeranforderungen für das Programm an erreichbare Maschinen weitergeleitet. In einem zentralisierten Dateisystem verursacht der Verlust der zentralen Dateispeichermaschine den Absturz des gesamten Systems.

© Copyright IBM Corp. 1989, 2000

- Gestiegene Effizienz: In einem verteilten Dateisystem wird die Auslastung über viele kleinere Datei-Server-Maschinen verteilt, die damit besser ausgelastet werden als eine größere (und für gewöhnlich teurere) Dateispeichermaschine eines zentralisierten Dateisystems.

Daß AFS ein verteiltes System ist, ist von außen nicht erkennbar, und so erscheint die Arbeit mit AFS-Dateien, als wären sie auf Ihrer lokalen Maschine gespeichert, mit der Ausnahme, daß Sie auf viel mehr Dateien zugreifen können. Und weil AFS auf die Leistungsfähigkeit der Client-Maschinen der Benutzer angewiesen ist, verringert eine steigende Anzahl von AFS-Benutzern die AFS-Leistung nicht nennenswert und macht es damit zu einer sehr effizienten Datenverarbeitungsumgebung.

AFS-Dateibereich und lokaler Dateibereich

AFS agiert als eine Erweiterung des lokalen UNIX-Dateisystems Ihrer Maschine. Ihr Systemadministrator erstellt auf der lokalen Platte ein Verzeichnis für jede AFS-Client-Maschine, damit sie als ein Gateway zu AFS fungieren kann. Gemäß Konvention wird dieses Verzeichnis **/afs** genannt, und es fungiert als das Stammverzeichnis des *AFS-Dateibereichs*.

Wie auch das UNIX-Dateisystem verwendet AFS eine hierarchische Dateistruktur (eine Baumstruktur). Unter dem Stammverzeichnis **/afs** befinden sich Unterverzeichnisse, die durch Ihren Systemadministrator angelegt werden, einschließlich Ihrem Ausgangsverzeichnis. Andere Verzeichnisse, die auf derselben Ebene wie **/afs** angesiedelt sind, wie **/usr**, **/etc** oder **/bin**, können sich entweder auf Ihrer lokalen Platte befinden oder Verknüpfungen zu AFS-Verzeichnissen sein. Dateien, die nur für die lokale Maschine relevant sind, werden für gewöhnlich auf der lokalen Maschine abgelegt. Alle anderen Dateien können in AFS gespeichert werden, und ermöglichen es damit vielen Benutzern, sie gemeinsam zu verwenden und halten den Plattenspeicherplatz der lokalen Maschine für andere Zwecke frei.

Anmerkung: Sie können AFS-Befehle nur für Dateien im AFS-Dateibereich verwenden oder für die lokalen Verzeichnisse, die Verknüpfungen zum AFS-Dateibereich sind.

Zellen und Standorte

Die Verwaltungsdomäne in AFS ist die *Zelle*. Die Administratoren jeder Zelle bestimmen, wie Client-Maschinen konfiguriert werden und wieviel Speicherplatz jedem Benutzer zur Verfügung gestellt wird. Die mit einer Zelle korrespondierende Organisation kann eine Firma, eine Abteilung einer Universität oder eine definierte Gruppe von Benutzern sein. Aus Sicht der Hardware ist eine Zelle eine Zusammenfassung von Client-Maschinen und Server-Maschinen, die per Definition zu derselben Zelle gehören. Ein AFS-*Standort* ist eine Zusammenfassung von einer oder mehreren zusammengehörigen Zellen. Zum Beispiel bilden die Zellen der ABC Corporation einen einzigen Standort.

Gemäß Konvention sind die Unterverzeichnisse des Verzeichnisses **/afs** zelluläre Dateibereiche, von denen jeder Unterverzeichnisse und Dateien enthält, die zu einer einzelnen Zelle gehören. Zum Beispiel werden Verzeichnisse und Dateien, die für die Zelle ABC Corporation relevant sind, im Unterverzeichnis **/afs/abc.com** abgelegt.

Während jede Zelle ihren eigenen Dateibereich organisiert und verwaltet, kann sie auch Verbindung zum Dateibereich anderer AFS-Zellen aufnehmen. Damit entsteht ein riesiger Dateibereich, der einen gemeinsamen Dateizugriff innerhalb und zwischen Zellen ermöglicht.

Die Zelle, zu der Ihre Client-Maschine gehört, wird als Ihre *lokale Zelle* bezeichnet. Alle anderen Zellen im AFS-Dateibereich heißen *fremde Zellen*.

Volumes und Mount-Punkte

Die Speicherplatten in einem Computer werden in Sektionen geteilt, die als *Partitionen* bezeichnet werden. AFS teilt darüberhinaus Partitionen in Einheiten, genannt *Volumes*, von denen jede eine untergeordnete Baumstruktur von zusammengehörenden Dateien und Verzeichnisses enthält. Das Volume stellt einen geeigneten Container für das Speichern zusammengehörender Dateien und Verzeichnisse dar. Ihr Systemadministrator kann, ohne daß Sie es bemerken, Volumes von der einen Datei-Server-Maschine zu einer anderen verschieben, da AFS die Position eines Volumes automatisch verfolgt.

Auf den Inhalt eines Volumes greifen Sie durch Zugriff auf seinen *Mount-Punkt* im AFS-Dateibereich zu. Ein Mount-Punkt ist ein spezielles Element des Dateisystems, das wie ein reguläres UNIX-Verzeichnis aussieht und agiert, jedoch AFS den Namen des Volumes mitteilt. Wenn Sie in ein anderes Verzeichnis wechseln (zum Beispiel mit Hilfe des Befehls **cd**), *kreuzen* Sie manchmal einen Mount-Punkt und starten den Zugriff auf den Inhalt eines anderen Volumes als zuvor. Sie bemerken aber normalerweise dieses Kreuzen nicht, weil AFS Mount-Punkte automatisch interpretiert und den Inhalt des neuen Verzeichnisses vom entsprechenden Volume abruft. Sie brauchen nicht zu verfolgen, welches Volume, welche Partition oder Datei-Server-Maschine den Inhalt eines Verzeichnisses enthält. Wenn Sie jedoch daran interessiert sind, können Sie den Speicherort eines Volumes herausfinden; Anweisungen finden Sie in „Suchen von Dateien und Verzeichnissen” auf Seite 28.

Wenn sich Ihr Systemadministrator an die herkömmliche Verfahrensweise gehalten hat, korrespondiert Ihr Ausgangsverzeichnis mit einem Volume, dessen gesamter Inhalt sich auf einer Partition einer Datei-Server-Maschine befindet. Benutzer-Volumes werden typischerweise mit **user.***username* benannt. Zum Beispiel wird das Volume für einen Benutzer namens **smith** in der Zelle **abc.com** als **user.smith** bezeichnet und gehört zum Verzeichnis **/afs/abc.com/usr/smith**.

Weil AFS-Volumes auf verschiedenen Datei-Server-Maschinen gespeichert werden, sind, wenn eine Maschine nicht mehr verfügbar ist, nur die Volumes auf dieser Maschine nicht mehr erreichbar. Volumes auf anderen Maschinen sind weiterhin erreichbar. Wenn sich jedoch der Mount-Punkt eines Volumes auf einem Volume befindet, der auf einer nicht erreichbaren Maschine gespeichert ist, ist das vorherige Volume ebenfalls nicht erreichbar. Aus diesem Grund werden Volumes, die häufig verwendete Verzeichnisse (zum Beispiel **/afs** und **/afs/***cellname*) enthalten, mehrfach kopiert und auf viele Datei-Server-Maschinen verteilt.

Quoten von Volumes

Jedes Volume hat eine Größenbegrenzung oder *Quote*, die durch den Systemadministrator festgelegt wird. Die Quote eines Volumes bestimmt die maximale Größe an Plattenspeicherplatz, die das Volume verbrauchen kann. Wenn Sie versuchen, die Quote eines Volumes zu überschreiten, erhalten Sie eine Fehlernachricht. Anweisungen zum Überprüfen der Quote eines Volumes finden Sie in „Anzeigen der Quote eines Volumes” auf Seite 25.

Volumes haben vollständig unabhängige Quoten. Zum Beispiel das aktuelle Arbeitsverzeichnis **/afs/abc.com/usr/smith**, welches der Mount-Punkt für das Volume **user.smith** mit 1000 freien Blöcken ist. Sie versuchen, eine 500 Blöcke große Datei aus dem aktuellen Arbeitsverzeichnis in das Verzeichnis **/afs/abc.com/usr/pat** zu kopieren, dem Mount-Punkt für das Volume **user.pat**. Sie erhalten jedoch eine Fehlernachricht, die mitteilt, daß nicht genug Speicherbereich vorhanden ist. Sie überprüfen die Quote des Volumes **user.pat** und erfahren, daß das Volume nur 50 freie Blöcke hat.

Verwenden von Dateien in AFS

Der Cache Manager

Sie können auf den AFS-Dateibereich nur während der Arbeit auf einer AFS-Client-Maschine zugreifen. Der *Cache Manager* auf dieser Maschine ist Ihr Agent für den Zugriff auf Informationen, die im AFS-Dateibereich gespeichert sind. Wenn Sie auf eine Datei zugreifen, fordert der Cache Manager auf Ihrer Client-Maschine die Datei von der entsprechenden Datei-Server-Maschine an und speichert (*zwischenspeichert*) eine Kopie davon auf der lokalen Platte Ihrer Client-Maschine. Anwendungsprogramme auf Ihrer Client-Maschine nutzen die lokale, zwischengespeicherte Kopie der Datei. Dies verbessert die Leistung, weil es viel schneller ist, eine lokale Datei zu verwenden als Anforderungen für Daten quer durch das Netzwerk zur Datei-Server-Maschine zu senden.

Weil Anwendungsprogramme die im Cache befindliche Kopie einer Datei verwenden, werden von Ihnen vorgenommenen Änderungen bis zum Schließen der Datei nicht dauerhaft in der zentralen Version gespeichert, die sich auf der Datei-Server-Maschine befindet. Beim Schließen schreibt der Cache

Manager Ihre Änderungen auf die Datei-Server-Maschine, wo sie die entsprechenden Teile der vorhandenen Datei ersetzen. Einige Anwendungsprogramme schließen eine Datei jedesmal, wenn Sie deren Sicherungsbefehl **save** eingeben (und danach sofort die Datei erneut öffnen, so daß Sie weiterarbeiten können). In anderen Programmen werden bei Eingabe des Befehls **save** die Änderungen nur in die im lokalen Cache befindliche Kopie geschrieben. Wenn Sie einen modernen Texteditor verwenden, müssen Sie die Datei regelmäßig schließen, um sicherzugehen, daß Ihre Änderungen dauerhaft gespeichert werden.

Wenn eine Datei-Server-Maschine nicht mehr erreichbar ist, können Sie die Arbeit mit der lokalen, zwischengespeicherten Kopie einer Datei, die von dieser Maschine abgerufen wurde, zwar fortsetzen, Sie können jedoch Ihre Änderungen nicht dauerhaft speichern, bis die Server-Maschine wieder verfügbar ist.

Aktualisieren der Kopien von im Cache befindlichen Dateien

Wenn die zentrale Version einer Datei auf der Datei-Server-Maschine verändert wird, teilt der AFS-Prozeß *File Server* auf dieser Maschine allen anderen Cache Managern mit Kopien dieser Datei mit, daß deren Version nicht länger gültig ist. AFS besitzt einen speziellen Mechanismus, um diese Mitteilungen effizient zu realisieren. Wenn der File Server dem Cache Manager eine Kopie einer veränderbaren Datei sendet, sendet er gleichzeitig einen *Rückruf*. Ein Rückruf stellt eine Zusage des File Servers dar, den Cache Manager zu kontaktieren, wenn die zentral gespeicherte Kopie der Datei während ihrer Benutzung verändert wird. Wenn dies geschieht, *unterbricht* der File Server den Rückruf. Wenn Sie ein Programm ausführen, das Daten von der veränderten Datei anfordert, nimmt der Cache Manager den unterbrochenen Rückruf an und erhält vom File Server eine aktualisierte Kopie der Datei. Rückrufe gewährleisten, daß Sie mit der jeweils aktuellen Kopie einer Datei arbeiten können.

Anmerkung: Der Rückrufmechanismus garantiert nicht, daß Sie die von irgend jemandem vorgenommenen Änderungen der Datei, die Sie verwenden, sofort erkennen. Ihr Cache Manager beachtet den unterbrochenen Rückruf nicht, bis Ihr Anwendungsprogramm von ihm weitere Daten aus der Datei anfordert.

Wenn mehrere Benutzer Dateien verändern

Wie ein Standard-UNIX-Dateisystem behält AFS nur die Änderungen einer Datei, die zuletzt gesichert wurden, ungeachtet dessen, wer die Änderungen vorgenommen hat. Wenn mehrere Benutzer mit denselben Dateien arbeiten, müssen Sie Ihre Arbeit koordinieren, um ein gegenseitiges Überschreiben der Änderungen zu vermeiden. Sie können AFS-ACLs (ACL = Access Control List, Zugriffssteuerungsliste) verwenden, um die Möglichkeiten anderer Benutzer, auf Ihre Dateien zuzugreifen oder sie zu verändern, einzuschränken

und sie somit am unbeabsichtigten Überschreiben Ihrer Dateien zu hindern. Siehe „Kapitel 4. Zugriffsschutz für Verzeichnisse und Dateien” auf Seite 33.

AFS-Sicherheit

AFS erleichtert es, daß viele Benutzer auf dieselben Dateien zugreifen, verwendet aber auch mehrere Mechanismen, um zu gewährleisten, daß nur berechtigte Benutzer auf den AFS-Dateibereich zugreifen. Diese Mechanismen sind:

- Kennwörter und gegenseitige Authentifizierung gewährleisten, daß nur berechtigte Benutzer auf den AFS-Dateibereich zugreifen
- Zugriffssteuerungslisten ermöglichen es den Benutzern, den Zugriff auf ihre eigenen Verzeichnisse zu verhindern oder zu gestatten

Kennwörter und gegenseitige Authentifizierung

AFS verwendet zwei zusammengehörende Mechanismen, um zu gewährleisten, daß nur berechtigte Benutzer auf den Dateibereich zugreifen: Kennwörter und gegenseitige Authentifizierung. Beide Mechanismen erfordern, daß ein Benutzer oder eine Benutzerin seine oder ihre Identität nachweist.

Wenn Sie sich erstmals gegenüber AFS identifizieren, müssen Sie das Ihrem Benutzernamen zugeordnete Kennwort angeben, um nachzuweisen, daß Sie sind, wer Sie vorgeben zu sein. Wenn Sie das korrekte Kennwort angeben, werden Sie *authentifiziert* und Ihr Cache Manager erhält ein *Token*. Ein Token ist ein Informationspaket, das durch ein AFS-Authentifizierungsprogramm verwürfelt worden ist, wobei Ihr Kennwort als Schlüssel verwendet wurde. Ihr Cache Manager kann das Token entwürfeln, weil er Ihr Kennwort und die Verwürfelungsmethode von AFS kennt.

Das Token dient gegenüber AFS-Server-Programmen als Nachweis, daß Sie als gültiger AFS-Benutzer authentifiziert sind. Es dient als Basis für die zweite Methode, mit deren Hilfe AFS Sicherheit gewährleistet, genannt *gegenseitige Authentifizierung*. Bei der gegenseitigen Authentifizierung, weisen beide Teilnehmer, die über das Netzwerk miteinander kommunizieren, einander ihre Identität nach. AFS erfordert eine gegenseitige Authentifizierung jedesmal, wenn ein Server und ein Client (meistens ein Cache Manager) miteinander kommunizieren.

Das Protokoll der gegenseitigen Authentifizierung, das AFS verwendet, wurde so gestaltet, daß es sehr schwer ist, sich in betrügerischer Absicht zu authentifizieren. Wenn Ihr Cache Manager in Ihrem Namen einen File Server kontaktiert, sendet er das Token, das Sie bei Ihrer Authentifizierung erhalten haben. Das Token wird mit einem Schlüssel verschlüsselt, den nur ein AFS File Server kennen kann. Wenn der File Server Ihr Token entschlüsseln kann, kann er mit Ihrem Cache Manager kommunizieren. Andererseits akzeptiert der Cache

Manager den File Server als echt, weil der File Server die Informationen im Token entschlüsseln und verwenden kann.

Zugriffssteuerungslisten

AFS verwendet *Zugriffssteuerungslisten* (*ACLs*), um zu bestimmen, wer auf die Informationen im AFS-Dateibereich zugreifen kann. Jedes AFS-Verzeichnis besitzt eine ACL, um anzugeben, welche Aktionen die verschiedenen Benutzer bezüglich dieses Verzeichnisses und seiner Dateien ausführen kann. Eine ACL kann bis zu 20 Einträge für Benutzer, Gruppen oder beide enthalten; jeder Eintrag enthält einen Benutzer oder eine Gruppe und die zugehörigen Berechtigungen.

Die Eigner eines Verzeichnisses sowie die Systemadministratoren haben auf eine ACL immer Zugriff. Den Benutzern gehören automatisch ihre Ausgangsverzeichnisse und Unterverzeichnisse. Andere Benutzer können die ACL eines Verzeichnisses nur definieren, wenn Ihnen diese Berechtigung für die ACL ausdrücklich erteilt wurde. Weitere Informationen zu ACLs finden Sie in „Kapitel 4. Zugriffsschutz für Verzeichnisse und Dateien” auf Seite 33.

Eine Gruppe wird von einem oder mehreren Benutzern und Client-Maschinen gebildet. Wenn ein Benutzer zu einer Gruppe gehört, die in einer ACL erscheint, erhält der Benutzer alle Berechtigungen, die dieser Gruppe erteilt wurden, so als wäre der Benutzer direkt in der ACL aufgeführt. In ähnlicher Weise besitzt ein Benutzer alle Berechtigungen, die einer Gruppe erteilt wurden, wenn er sich bei einer Client-Maschine angemeldet hat, die zu dieser Gruppe gehört. Anweisungen zum Definieren und Verwenden von Gruppen finden Sie in „Kapitel 5. Verwendung von Gruppen” auf Seite 53.

Alle Benutzer, die auf den Dateibereich Ihrer Zelle zugreifen können, authentifiziert oder nicht, werden automatisch einer Gruppe mit der Bezeichnung **system:anyuser** zugeordnet. Eine Beschreibung dazu, wie die Gruppe **system:anyuser** in ACLs untergebracht wird, finden Sie in „Erweitern des Zugriffs auf Benutzer fremder Zellen” auf Seite 40.

Anmerkung: Sie können die UNIX-Modusbits verwenden, um den Zugriff auf spezielle Dateien innerhalb eines AFS-Verzeichnisses zu steuern; jedoch ist die Wirkung dieser Modusbits unter AFS anders als im Standard-UNIX-Dateisystem. Siehe „Zugriffsschutz für Dateien und Verzeichnisse” auf Seite 9.

Unterschiede zwischen UNIX und AFS

AFS ist ähnlich dem UNIX-Dateisystem gestaltet. Zum Beispiel sind viele der UNIX-Basisbefehle zur Dateimanipulation (**cp** für kopieren, **rm** für entfernen und so weiter) in AFS dieselben wie in UNIX. Alle Ihre Anwendungsprogramme arbeiten wie vorher. Die folgenden Abschnitte beschreiben einige der Unterschiede zwischen einem Standard-UNIX-Dateisystem und AFS.

Gemeinsamer Dateizugriff

AFS ermöglicht es den Benutzern, ferne Dateien genauso einfach gemeinsam zu benutzen wie lokale Dateien. Um in AFS auf eine Datei auf einer fernen Maschine zuzugreifen, geben Sie einfach den Pfadnamen der Datei an. Im Gegensatz dazu müssen Sie, um auf eine Datei im UNIX-Dateisystem einer fernen Maschine zuzugreifen, sich bei der fernen Maschine anmelden oder auf der lokalen Maschine einen Mount-Punkt erstellen, der auf ein Verzeichnis im UNIX-Dateisystem der fernen Maschine weist.

AFS-Benutzer können alle Dateien im Stammverzeichnis **/afs**, die die entsprechenden Berechtigungen besitzen, gemeinsam benutzen. Ein AFS-Benutzer, der die notwendigen Berechtigungen besitzt, kann auf eine Datei in jeder AFS-Zelle einfach durch Angabe des Pfadnamens der Datei zugreifen. Der gemeinsame Dateizugriff in AFS ist nicht durch geografische Entfernungen oder Unterschiede in den Betriebssystemen eingeschränkt.

Anmelden und Authentifizierung

Um ein authentifizierter AFS-Benutzer zu werden, müssen Sie AFS ein Kennwort liefern.

- Auf Maschinen, die ein für AFS modifiziertes Anmeldedienstprogramm verwenden, wird Anmelden und Authentifizieren in einem Schritt durchgeführt; Ihre Erstanmeldung authentifiziert Sie automatisch bei AFS.
- Auf Maschinen, die ein für AFS modifiziertes Anmeldedienstprogramm nicht verwenden, werden Anmelden und Authentifizieren in zwei Schritten durchgeführt.
  1. Melden Sie sich bei Ihrer lokalen Maschine an.
  2. Geben Sie den Befehl **klog** mit dem Argument **-setpag** ein, um sich bei AFS zu authentifizieren und Ihr Token zu erhalten.

Ihr Systemadministrator kann Ihnen sagen, ob Ihre Maschine ein für AFS modifiziertes Anmeldedienstprogramm verwendet oder nicht. Weitere Anweisungen zum Anmelden finden Sie in „Anmelden und Authentifizieren bei AFS” auf Seite 13.

AFS-Authentifizierungskennwörter werden eher in einer speziellen AFS-Datenbank als in der lokalen Kennwortdatei (**/etc/passwd** oder ähnliches) gespeichert. Wenn Ihre Maschine ein für AFS modifiziertes Anmeldedienstprogramm verwendet, können Sie Ihr Kennwort mit einem einzigen Befehl

ändern. Wenn Ihre Maschine ein für AFS modifiziertes Anmeldedienstprogramm nicht verwendet, müssen Sie mehrere Befehle eingeben, um Ihr AFS- und Ihr lokales Kennwort zu ändern. Siehe „Ändern Ihres Kennworts” auf Seite 22.

Zugriffsschutz für Dateien und Verzeichnisse

AFS ist nicht auf den Modusbit-Zugriffsschutz eines Standard-UNIX-Systems angewiesen (obwohl sein Zugriffsschutzsystem mit diesen Modusbits interagiert). Statt dessen verwendet AFS eine Zugriffssteuerungsliste (ACL), um den Zugriff auf jedes Verzeichnis und seinen Inhalt zu steuern. Die folgende Liste faßt die Unterschiede zwischen den zwei Methoden zusammen:

- UNIX-Modusbits geben drei Typen von Zugriffsberechtigungen an: **r** (**read**), **w** (**write**) und **x** (**execute**). Eine AFS-ACL verwendet sieben Berechtigungstypen: **r** (**read**), **l** (**lookup**), **i** (**insert**), **d** (**delete**), **w** (**write**), **k** (**lock**) und **a** (**administer**). Weitere Informationen finden Sie unter „AFS-ACL-Berechtigungen” auf Seite 34 und „Verwendung der UNIX-Modusbits durch AFS” auf Seite 50.
- Die drei Gruppen von Modusbits für jede UNIX-Datei oder jedes UNIX-Verzeichnis ermöglichen es Ihnen, Berechtigungen an drei Benutzer oder Benutzergruppen zu erteilen: Dem Eigner der Datei oder des Verzeichnisses, der Gruppe, der die Datei oder das Verzeichnis gehört, und allen anderen Benutzern. Eine ACL kann bis zu 20 Einträge aufnehmen, von denen jeder bestimmte Berechtigungen für einen Benutzer oder eine Gruppe definiert. Anders als in Standard-UNIX kann ein Benutzer zu einer beliebigen Anzahl von Gruppen gehören, und Gruppen können sowohl durch Benutzer als auch durch Systemadministratoren definiert werden. Siehe „Kapitel 5. Verwendung von Gruppen” auf Seite 53.
- Die UNIX-Modusbit werden individuell für jede Datei und jedes Verzeichnis gesetzt. Eine ACL bezieht sich auf alle Dateien in einem Verzeichnis. Während auf den ersten Blick die AFS-Methode weniger präzise erscheint, gibt es tatsächlich (bei geeigneter Verzeichnisstruktur) keine gravierenden Nachteile gegenüber dem Zugriffsschutz auf Verzeichnisebene, wobei sie leichter zu erstellen und zu verwalten sind.

Maschinenausfälle

Die Störungen, die Sie beim Ausfall eines Standard-UNIX-Dateisystems erleben, sind von anderer Art als wenn ein oder mehrere selbständige AFS-Datei-Server-Maschinen nicht mehr erreichbar sind. Wenn ein Standard-UNIX-Dateisystem ausfällt, wird das System einfach gesperrt, und Sie können alle Änderungen in gerade bearbeiteten Dateien verlieren.

Wenn eine AFS-Datei-Server-Maschine ausfällt, können Sie auf die Dateien auf dieser Maschine nicht zugreifen. Wenn jedoch eine Kopie der Datei von einer anderen Datei-Server-Maschine verfügbar ist, kann es sein, daß Sie den Ausfall des Servers nicht einmal bemerken. Damit gibt AFS dem Systemadministrator Ihrer Zelle die Möglichkeit, Kopien allgemein zugänglicher Programme

auf mehreren Datei-Servern zu speichern. Der Cache Manager wählt unter den Kopien automatisch; wenn eine Kopie nicht mehr verfügbar ist, wählt der Cache Manager einfach eine andere.

Wenn von einer Datei, die auf einer ausgefallenen Server-Maschine gespeichert ist, keine anderen Kopien vorhanden sind, können Sie für gewöhnlich die Arbeit mit der Kopie fortsetzen, die sich im lokalen AFS-Cache Ihrer Client-Maschine befindet. Sie können jedoch die Änderungen der Dateien, die in einer ausgefallenen Datei-Server-Maschine gespeichert sind, nicht sichern, bis diese wieder erreichbar ist.

Ferne Befehle

Die *fernen Befehle* von UNIX ermöglichen es Ihnen, Programme auf einer fernen Maschine mit Hilfe eines Programms wie **Telnet** auszuführen, ohne eine Verbindung mit ihr herstellen zu müssen. Viele der fernen Befehle (wie **ftp**, **rcp** und **rsh**) sind auch in AFS verfügbar, je nachdem, wie sie durch Ihren Administrator konfiguriert wurden. Wenn die ferne Maschine einen Cache Manager hat, wird Ihr Token dort ebenfalls verwendet, und Sie werden authentifiziert, während der ferne Befehl läuft. Wenn die ferne Maschine keinen Cache Manager hat, erhalten Sie die folgende Nachricht:

```
Warning: unable to authenticate.
```

In diesem Fall werden Sie beim UNIX-Dateisystem der fernen Maschine angemeldet, wobei Sie gegenüber AFS nicht authentifiziert sind. Sie können auf die lokalen Dateien auf der fernen Maschine zugreifen und auf die AFS-Verzeichnisse, die den Zugriff auf die Gruppe **system:anyuser** gestatten, jedoch nicht auf geschützte AFS-Verzeichnisse.

Unterschiede in der Semantik von Standard-UNIX-Befehlen

Dieser Abschnitt faßt die Unterschiede in der Funktionalität einiger allgemein verwendeter UNIX-Befehle zusammen.

chmod
: Ausschließlich Mitglieder der Gruppe **system:administrators** können diesen Befehl verwenden, um die Modusbits setuid, setgid oder sticky für AFS-Dateien zu setzen. (Weitere Informationen zu dieser Gruppe finden Sie in „Verwenden von Systemverwaltungsgruppen in ACLs” auf Seite 38.)

chown
: Ausschließlich Mitglieder der Gruppe **system:administrators** können diesen Befehl für AFS-Dateien verwenden.

chgrp
: Ausschließlich Mitglieder der Gruppe **system:administrators** können diesen Befehl für AFS-Dateien und -Verzeichnisse verwenden.

groups
: Wenn die AFS-Token des Benutzers durch eine Prozeßauthentifizie-

rungsgruppe (PAG) definiert werden, enthält die Ausgabe dieses Befehls zwei größere Nummern. Eine Beschreibung von PAGs finden Sie in „Authentifizieren bei AFS" auf Seite 14.

inetd Die AFS-Version dieses Dämons authentifiziert ferne Benutzer der für AFS modifizierten Befehle **rcp** und **rsh** bei AFS.

Anmeldedienstprogramme
Für AFS modifizierte Anmeldedienstprogramme melden Sie beim lokalen UNIX-Dateisystem an und authentifizieren Sie bei AFS.

ln Sie können diesen Befehl nicht verwenden, um eine feste Verbindung zwischen Dateien, die sich in verschiedenen AFS-Verzeichnissen befinden, herzustellen. Sie müssen die Option **-s** hinzufügen, um statt dessen eine symbolische Verbindung zu erstellen.

Verwendung von AFS mit NFS

Einige Zellen verwenden zusätzlich zu AFS das Networking File System (NFS). Wenn Sie auf einer NFS-Client-Maschine arbeiten, kann Ihr Systemadministrator sie so konfigurieren, daß sie auf den AFS-Dateibereich mit Hilfe des Programms *NFS/AFS Translator*™ zugreift. Siehe „Anhang A. Verwenden des NFS / AFS Translator" auf Seite 75.

Kapitel 2. Verwendung von AFS

Dieses Kapitel erklärt, wie die folgenden vier AFS-Grundfunktionen auszuführen sind: Anmelden und Authentifizieren bei AFS, Beenden einer AFS-Sitzung, Zugreifen auf den AFS-Dateibereich und Ändern Ihres Kennworts.

Anmelden und Authentifizieren bei AFS

Um auf den AFS-Dateibereich als ein authentifizierter Benutzer zugreifen zu können, müssen Sie sich sowohl in einem lokalen UNIX-Dateisystem einer AFS-Client-Maschine anmelden als auch bei AFS authentifizieren. Beim Anmelden etablieren Sie Ihre lokale Systemidentität. Beim Authentifizieren weisen Sie Ihre Identität gegenüber AFS nach und erhalten ein Token, das Ihr Cache Manager verwendet, um gegenüber den AFS-Server-Prozessen, mit denen er in Ihrem Namen Kontakt aufnimmt, Ihren authentifizierten Status nachzuweisen. Nicht authentifizierte Benutzer (die kein Token besitzen) haben auf AFS-Verzeichnisse und -Dateien nur begrenzten Zugriff.

Anmelden

Auf Maschinen, die ein für AFS modifiziertes Anmeldedienstprogramm verwenden, wird Anmelden und Authentifizieren in einem Schritt durchgeführt. Auf Maschinen, die ein für AFS modifiziertes Anmeldedienstprogramm nicht verwenden, werden Anmelden und Authentifizieren in mehreren Schritten durchgeführt. Um den Typ des Anmeldedienstprogramms auf Ihrer Maschine zu ermitteln, können Sie nach dem Anmelden auf AFS-Token prüfen oder Ihren Systemadministrator fragen, der Ihnen die Unterschiede zwischen Ihrem Anmeldeverfahren und den zwei hier beschriebenen Methoden ebenfalls erläutern kann.

So melden Sie sich mit Hilfe eines für AFS modifizierten Anmeldedienstprogramms an

Geben Sie Ihren Benutzernamen an der Eingabeaufforderung `login:` ein, die erscheint, wenn Sie eine neue Verbindung zu einer Maschine herstellen. Geben Sie danach Ihr Kennwort an der Eingabeaufforderung `Password:`, wie im folgenden Beispiel dargestellt, ein. (Ihr Kennwort wird auf dem Bildschirm nicht sichtbar wiedergegeben.)

```
    login: username
Password: password
```

Wenn Sie sich nicht sicher sind, welcher Typ eines Anmeldedienstprogramms auf Ihrer Maschine läuft, verwenden Sie am besten den Befehl **tokens**, um zu prüfen, ob Sie authentifiziert sind; Anweisungen finden Sie in „So lassen Sie

© Copyright IBM Corp. 1989, 2000

sich Ihre Token anzeigen" auf Seite 17. Wenn Sie kein Token besitzen, geben Sie den Befehl **klog**, wie in „So authentifizieren Sie sich bei AFS" auf Seite 16 beschrieben, ein.

So melden Sie sich mit Hilfe einer aus zwei Schritten bestehenden Anmeldeprozedur an

Wenn Ihre Maschine über kein für AFS modifiziertes Anmeldedienstprogramm verfügt, müssen Sie eine aus zwei Schritten bestehende Prozedur ausführen:

1. Melden Sie sich beim lokalen Dateisystem Ihrer Client-Maschine mittels Benutzername und Kennwort an der Eingabeaufforderung **login** des Programms an.
2. Authentifizieren Sie sich bei AFS mit Hilfe des Befehls **klog**. Verwenden Sie das Argument **-setpag** des Befehls, um Ihr Token mit einer speziellen Identifikationsnummer, genannt *PAG* (für *Prozeßauthentifizierungsgruppe*), zu verknüpfen. Eine Beschreibung von PAGs finden Sie in „Schützen Ihrer Token mit einer PAG" auf Seite 15.

   ```
   % klog -setpag
   Password: Ihr_AFS_Kennwort
   ```

Anmerkung: Wenn Ihre Maschine eine aus zwei Schritten bestehende Anmeldeprozedur verwendet, können Sie für das Anmelden und Authentifizieren zwei verschiedene Kennwörter wählen. Die einfachste Variante ist jedoch die Verwendung von nur einem Kennwort für beides. Sprechen Sie mit Ihrem Systemadministrator.

Authentifizieren bei AFS

Um im AFS-Dateibereich so effektiv wie möglich arbeiten zu können, müssen Sie bei AFS authentifiziert werden. Dabei wird Ihrem Cache Manager als Nachweis für Ihren authentifizierten Status ein Token übergeben. Er verwendet Ihr Token beim Anfordern von Services von AFS-Servern, die das Token als Nachweis für Ihren authentifizierten Status akzeptieren. Wenn Sie kein Token besitzen, werden Sie von AFS-Servern als **anonymer** Benutzer betrachtet, womit Ihr Zugriff auf den AFS-Dateibereich eingeschränkt wird: Sie verfügen in diesem Fall nur über die ACL-Berechtigungen, die der Gruppe **system:anyuser** erteilt wurden.

Sie können jederzeit neue Token (neu authentifizieren) erhalten, auch nach dem Einsatz eines für AFS modifizierten Anmeldedienstprogramms, mit dem Sie sich in einem Schritt anmelden und authentifizieren. Geben Sie den Befehl **klog**, wie in „So authentifizieren Sie sich bei AFS" auf Seite 16 beschrieben, ein.

Schützen Ihrer Token mit einer PAG

Um Ihren Zugriff auf AFS so sicher wie möglich zu gestalten, verknüpfen Sie am besten Ihre Token mit einer eindeutigen Identifikationsnummer, genannt *PAG* (für *Prozeßauthentifizierungsgruppe*), zu verknüpfen. Für AFS modifizierte Anmeldedienstprogramme erstellen automatisch eine PAG und verknüpfen die neuen Token mit ihr. Um eine PAG beim Verwenden einer aus zwei Schritten bestehenden Anmeldeprozedur zu erstellen, verwenden Sie zum Befehl **klog** dessen Markierung **-setpag**. Wenn Sie diese Markierung nicht verwenden, werden Ihre Token statt dessen mit Ihrer UNIX-UID-Nummer verknüpft. Diese Art der Zuordnung hat insbesondere zwei Nachteile:

- Jeder, der Ihre lokale UNIX-Identität annehmen kann, kann Ihre Token benutzen. Der lokale Superuser **root** kann stets den UNIX-Befehl **su** verwenden, um Ihre UNIX-UID anzunehmen, auch ohne Ihr Kennwort zu kennen.
- In einigen Umgebungen können bestimmte Programme Ihre Token nicht verwenden, auch wenn es für sie angebracht wäre. Zum Beispiel können Druckbefehle wie **lp** oder **lpr** möglicherweise auf die zu druckenden Dateien nicht zugreifen, weil sie Ihre Token nicht benutzen können.

Erlangen von Token für fremde Zellen

Ein Token ist nur in einer Zelle gültig (in der Zelle, deren AFS-Authentifizierungsservice es ausgegeben hat). Die AFS-Server-Prozesse in jeder anderen Zelle betrachten Sie als **anonymen** Benutzer, es sein denn, Sie besitzen in der Zelle einen Benutzereintrag und authentifizieren sich mit deren AFS-Authentifizierungsservice.

Um in einer fremden Zelle Token zu erlangen, verwenden Sie das Argument **-cell** zum Befehl **klog**. Sie können gleichzeitig Token für Ihre Home-Zelle und eine oder mehrere fremde Zellen besitzen.

Die Regel ″Ein Token pro Zelle″

Für jede PAG, die Sie von einer Client-Maschine erhalten haben, können Sie nur ein Token pro Zelle besitzen. Wenn Sie für eine bestimmte Zelle bereits ein Token besitzen und den Befehl **klog** eingeben, überschreibt das neue Token das vorhandene. Ein neues Token zu besorgen ist nützlich, wenn Ihr aktuelles Token fast abgelaufen ist, Sie aber die Arbeit mit AFS-Dateien fortsetzen möchten. Eine Beschreibung zum Auslaufen eines Tokens finden Sie in „Die Lebensdauer eines Tokens” auf Seite 16.

Um für dieselbe Zelle ein zweites Token zu erlangen, müssen Sie sich entweder auf einer anderen Maschine anmelden oder eine andere, getrennte Verbindung zu der Maschine herstellen, auf der Sie bereits ein Token besitzen (zum Beispiel mit Hilfe des Dienstprogramms **Telnet**). Für jede separate Maschine oder Verbindung erhalten Sie eine neue PAG und und können die zugehörigen Token nur bei der Arbeit auf dieser Maschine oder Verbindung benutzen.

Erlangen von Token als ein anderer Benutzer

Sie können sich mit einem anderen Benutzernamen authentifizieren, wenn Sie das zugehörige Kennwort kennen. (Es ist natürlich nicht in Ordnung, das Token eines anderen Benutzers ohne Berechtigung zu benutzen.) Wenn Sie den Befehl **klog** zur Authentifizierung mit einem anderen AFS-Benutzernamen verwenden, behalten Sie Ihre eigene (UNIX)-Identität, der AFS-Server-Prozeß erkennt Sie jedoch als den anderen Benutzer. Das neue Token ersetzt jedes Token, das Sie bereits für die betreffende Zelle besitzen (aus dem in „Die Regel ″Ein Token pro Zelle″” auf Seite 15 beschriebenen Grund).

Die Lebensdauer eines Tokens

Token haben eine begrenzte Lebensdauer. Um zu ermitteln, wann Ihre Token ablaufen, geben Sie den Befehl **tokens**, wie in „So lassen Sie sich Ihre Token anzeigen” auf Seite 17 beschrieben, ein. Wenn Sie auf AFS nicht mehr zugreifen können, obwohl dies normalerweise ging, erhalten Sie mittels des Befehls **tokens** eine Auskunft, ob ein abgelaufenes Token möglicherweise die Ursache ist.

Der Administrator Ihrer Zelle stellt die Standardlebensdauer Ihres Tokens ein. Der AFS-Authentifizierungsservice verleiht einem Token niemals eine Lebensdauer, die länger ist als die Standardeinstellung, jedoch können Sie ein Token mit einer kürzeren Lebensdauer anfordern. Auf der Referenzseite **klog** in der *AFS Administration Reference* erhalten Sie Informationen darüber, wie das Argument **-lifetime** dieses Befehls für diesen Zweck verwendet wird.

Authentifizieren für DFS-Zugriff

Wenn Ihre Maschine für den Zugriff auf den DFS-Dateibereich einer DCE-Zelle mit Hilfe des AFS/DFS Migration Toolkit konfiguriert ist, können Sie den Befehl **dlog** verwenden, um sich bei DCE zu authentifizieren. Der Befehl **dlog** hat keinen Einfluß auf Ihre Zugriffsmöglichkeiten auf den AFS-Dateibereich.

Wenn Ihr Systemadministrator ihren AFS-Benutzereintrag in einen DCE-Benutzereintrag umgewandelt hat und Sie sich Ihres DCE-Kennworts nicht sicher sind, verwenden Sie den Befehl **dpass**, um es sich anzeigen zu lassen. Sie müssen als der AFS-Benutzer authentifiziert sein, dessen AFS-Benutzereintrag in einen DCE-Benutzereintrag umgewandelt wurde, und Sie müssen das korrekte AFS-Kennwort kennen. Wie der Befehl **dlog** hat auch der Befehl **dpass** keine Funktionalität bezüglich AFS.

Weitere Informationen zum Verwenden der Befehle **dlog** und **dpass** gibt Ihnen Ihr Systemadministrator.

So authentifizieren Sie sich bei AFS

Wenn Ihre Maschine kein für AFS modifiziertes Anmeldedienstprogramm verwendet, müssen Sie sich authentifizieren, nachdem Sie sich mit Hilfe des

Befehls **klog** angemeldet haben. Sie können diesen Befehl auch jederzeit verwenden, um ein Token mit einem späteren Ablaufdatum als Ihr aktuelles Token zu erlangen.

```
   % klog [-setpag] [-cell <Zellenname>]
Password: Ihr_AFS_Kennwort
```

wobei

-setpag
: Verknüpft die auszugebenden Token mit einer PAG (siehe „Schützen Ihrer Token mit einer PAG" auf Seite 15). Bei der erstmaligen Verwendung dieser Markierung erhalten Sie ein Token für eine bestimmte Zelle während einer Anmeldesitzung oder-verbindung. Verwenden Sie sie nicht beim Aktualisieren des Tokens für eine Zelle während derselben Sitzung.

-cell
: Bezeichnet die Zelle, für die das Token ausgegeben werden soll. In der Zelle müssen Sie einen Benutzereintrag besitzen.

Ihr Kennwort wird auf dem Bildschirm nicht sichtbar widergegeben. Wenn die Eingabeaufforderung der Befehls-Shell wieder erscheint, sind Sie ein authentifizierter AFS-Benutzer. Sie können den Befehl **tokens** verwenden, um zu überprüfen, ob Sie authentifiziert sind, wie im folgenden Abschnitt beschrieben.

So lassen Sie sich Ihre Token anzeigen

Verwenden Sie den Befehl **tokens**, um sich Ihre Token anzeigen zu lassen.

```
   % tokens
```

Die folgende Ausgabe zeigt an, daß Sie keine Token besitzen:

```
   Tokens held by the Cache Manager:
--End of list--
```

Wenn Sie ein oder mehrere Token besitzen, ähnelt die Ausgabe in etwa der des folgenden Beispiels, in dem die Token für AFS UID 1022 in der Zelle **abc.com** am 03. August um 14:35 Uhr ablaufen. Die Token für AFS UID 9554 in der Zelle **stateu.edu** laufen am 04. August um 1:02 Uhr ab.

```
   Tokens held by the Cache Manager:
User's (AFS ID 1022) tokens for afs@abc.com [Expires Aug 3 14:35]
User's (AFS ID 9554) tokens for afs@stateu.edu [Expires Aug 4 1:02]
--End of list--
```

Beispiel: Authentifizieren in der lokalen Zelle

Angenommen, Benutzer **terry** kann eine Datei nicht sichern. Er verwendet den Befehl **tokens** und findet heraus, daß seine Token abgelaufen sind. Er authentifiziert sich in seiner lokalen Zelle unter seiner aktuellen Identität neu, indem er den folgenden Befehl eingibt:

```
   % klog
Password: Terrys_Kennwort
```

Danach gibt er den Befehl **tokens** ein, um sicherzustellen, daß er authentifiziert ist.

```
   % tokens
Tokens held by the Cache Manager:
User's (AFS ID 4562) tokens for afs@abc.com [Expires Jun 22 14:35]
--End of list--
```

Beispiel: Authentifizieren als ein anderer Benutzer

Jetzt authentifiziert sich **terry** in seiner lokalen Zelle als ein anderer Benutzer, und zwar als **pat**. Das neue Token ersetzt das vorhandene Token von **terry**, weil der Cache Manager nur ein Token pro Zelle und pro Anmeldesitzung auf einer Maschine speichern kann.

```
   % klog pat
Password: Pats_Kennwort
% tokens
Tokens held by the Cache Manager:
User's (AFS ID 4278) tokens for afs@abc.com [Expires Jun 23 9:46]
--End of list--
```

Beispiel: Authentifizieren in einer fremden Zelle

Jetzt authentifiziert sich **terry** in der Zelle **stateu.edu**, in der sein Benutzereintrag die Bezeichnung **ts09** trägt.

```
   % klog ts09 -cell stateu.edu
Password: ts09_Kennwort
% tokens
Tokens held by the Cache Manager:
User's (AFS ID 4562) tokens for afs@abc.com [Expires Jun 22 14:35]
User's (AFS ID 8346) tokens for afs@stateu.edu [Expires Jun 23 1:02]
--End of list--
```

Begrenzung von fehlgeschlagenen Authentifizierungsversuchen

Ihr Systemadministrator kann die Anzahl fehlgeschlagener Versuche bei der Eingabe des Kennworts während des Authentifizierens bei AFS (entweder mit Hilfe eines für AFS modifizierten Anmeldedienstprogramms oder des Befehls **klog**) festlegen. Wenn Sie die Grenze überschreiten, weist der AFS-Authentifizierungsservice weitere Authentifizierungsversuche für eine durch den Systemadministrator festgelegte Zeitspanne ab. Der Zweck dieser Begrenzung besteht darin, den Zugriff durch nicht autorisierte Benutzer auf Ihr Konto mittels einer Reihe von Kennwörtern zu verhindern.

Um zu ermitteln, ob Ihr Benutzerkonto mit einer solchen Begrenzung versehen ist, fragen Sie Ihren Systemadministrator oder verwenden Sie den Befehl **kas examine**, wie in „So lassen Sie sich die Begrenzung fehlgeschlagener Authentifizierungsversuche und die Sperrzeit anzeigen” auf Seite 19 beschrieben.

Die folgende Nachricht zeigt an, daß Sie die Grenze fehlgeschlagener Authentifizierungsversuche überschritten haben.

```
Unable to authenticate to AFS because ID is locked - see your system admin
```

So lassen Sie sich die Begrenzung fehlgeschlagener Authentifizierungsversuche und die Sperrzeit anzeigen

Verwenden Sie den Befehl **kas examine** um zu ermitteln, ob es eine Begrenzung der Anzahl erfolgloser Authentifizierungsversuche für Ihr Benutzerkonto und zugehörige Sperrzeiten gibt. Sie können jedoch nur Ihr eigenes Konto überprüfen. Die vierte Zeile der Ausgabe enthält die maximale Anzahl der Versuche, ein falsches Kennwort einzugeben, bevor Ihr Konto gesperrt wird. Das Feld Sperrzeit in der nächsten Zeile enthält die Angabe, wie lange der AFS-Authentifizierungsservice Authentifizierungsversuche zurückweist, nachdem die Grenze überschritten wurde.

```
% kas examine Ihr_Benutzername
Password for Ihr_Benutzername: Ihr_AFS_Kennwort
```

Das folgende Beispiel stellt die Ausgabe für den Benutzer **pat** dar, dem neun erfolglose Authentifizierungsversuche erlaubt sind. Die Sperrzeit beträgt 25,5 Minuten.

```
User data for pat
key (15) cksum is 3414844392, last cpw: Thu Oct 21 16:05:44 1999
password will expire: Fri Nov 26 20:44:36 1999
9 consecutive unsuccessful authentications are permitted.
The lock time for this user is 25.5 minutes.
User is not locked.
entry never expires. Max ticket lifetime 100.00 hours.
last mod on Wed Aug 18 08:22:29 1999 by admin
permit password reuse
```

Beenden einer AFS-Sitzung

Weil das Anmelden und Authentifizieren bei AFS unterschiedliche Operationen sind, müssen Sie sich beim Beenden einer AFS-Sitzung sowohl abmelden als auch deauthentifizieren (verwenden Sie den Befehl **unlog**, um Ihre Token zu löschen). Das einfache Abmelden zerstört nicht notwendigerweise Ihre Token.

Sie können den Befehl **unlog** jederzeit verwenden, wenn Sie sich deauthentifizieren möchten, und nicht nur beim Abmelden. Zum Beispiel ist es eine gute Verfahrensweise, sich zu deauthentifizieren, bevor Sie Ihre Maschine unbeaufsichtigt lassen, um zu verhindern, daß während Ihrer Abwesenheit andere Benutzer Ihre Token verwenden. Wenn Sie an Ihre Maschine zurückkehren, geben Sie den Befehl **klog** ein, um sich, wie in „So authentifizieren Sie sich bei AFS” auf Seite 16 beschrieben, neu zu authentifizieren.

Verwenden Sie den Befehl **unlog** nicht, wenn Sie Aufträge ausführen, die eine lange Zeit bis zu Ihrer Beendigung dauern, auch wenn Sie sich abmelden. Solche Prozesse müssen während der gesamten Zeit, in der Sie berechtigten Zugriff auf AFS benötigen, ein Token besitzen.

Wenn Sie Token von mehreren Zellen besitzen und nur einige davon löschen möchten, verwenden Sie zum Befehl **unlog** das Argument **-cell**.

So löschen Sie Token

Geben Sie den Befehl **unlog** ein, um Ihre Token zu löschen:

```
% unlog -cell <Zellenname>+
```

Lassen Sie das Argument **-cell** weg, um alle Ihre Token zu löschen, oder verwenden Sie es, um jede Zelle, für die Token gelöscht werden sollen, zu bezeichnen. Am besten ist es, den vollständigen Namen jeder Zelle anzugeben (wie **stateu.edu** oder **abc.com**).

Sie können den Befehl **tokens** verwenden, um zu überprüfen, ob Ihre Token zerstört wurden, wie im folgenden Beispiel.

```
% tokens
Tokens held by the Cache Manager:
--End of list--
```

Beispiel: Deauthentifizieren von einer speziellen Zelle

Im folgenden Beispiel besitzt eine Benutzerin Token sowohl in der Zelle **Buchhaltung** als auch in der Zelle **Marketing** ihrer Firma. Sie löscht das Token für die Zelle **acctg.abc.com**, behält jedoch das Token für die Zelle **mktg.abc.com**.

```
% tokens
Tokens held by the Cache Manager:
User's (AFS ID 35) tokens for afs@acctg.abc.com [Expires Nov 10 22:30]
User's (AFS ID 674) tokens for afs@mktg.abc.com [Expires Nov 10 18:44]
--End of list--
% unlog -cell acctg.abc.com
% tokens
Tokens held by the Cache Manager:
User's (AFS ID 674) tokens for afs@mktg.abc.com [Expires Nov 10 18:44]
--End of list--
```

So melden Sie sich ab

Nachdem Sie sich deauthentifiziert haben, melden Sie sich mit dem für den Typ Ihrer Maschine entsprechenden Befehl ab, der einer der folgenden sein kann.

```
% logout
```

oder

```
% exit
```

oder

```
% <Strg-d>
```

Zugreifen auf den AFS-Dateibereich

Während Sie angemeldet und authentifiziert sind, können Sie auf Dateien in AFS in derselben Weise zugreifen wie im UNIX-Dateisystem. Der einzige Unterschied besteht darin, daß Sie auf viel mehr Dateien zugreifen können. Aber wie auch im UNIX-Dateisystem können Sie nur auf die Dateien zugreifen, für die Sie die Berechtigung besitzen. AFS verwendet Zugriffssteuerungslisten (ACL = Access Control Lists) um den Zugriff zu steuern, wie in „Kapitel 4. Zugriffsschutz für Verzeichnisse und Dateien” auf Seite 33 beschrieben.

AFS-Pfadnamen

AFS-Pfadnamen sehen denen im UNIX-Dateisystem sehr ähnlich. Der Hauptunterschied besteht darin, daß jeder AFS-Pfadname mit dem AFS-Stammverzeichnis beginnt, das gemäß Konvention als **/afs** bezeichnet wird. Das **/afs** an der Spitze des Dateibereichs jeder AFS-Zelle verknüpft die einzelnen Dateibereiche zu einem globalen Dateibereich.

Hinweis für Windows-Benutzer: Windows verwendet einen umgekehrten Schrägstrich (\ ) anstatt eines normalen Schrägstrichs (/), um die Elemente in einem Pfadnamen voneinander zu trennen. Ansonsten gestaltet sich der Zugriff auf den AFS-Dateibereich in derselben Weise wie für Benutzer von UNIX-Maschinen.

Das zweite Element in AFS-Pfadnamen ist generell ein Zellenname. Zum Beispiel wird die Zelle ABC Corporation als **abc.com** bezeichnet, und der Pfadname jeder Datei in ihrem Dateibereich beginnt mit der Zeichenfolge **/afs/abc.com**. Einige Zellen erstellen auch ein Verzeichnis auf der zweiten Ebene mit einem verkürzten Namen (wie **abc** für **abc.com** oder **stateu** für **stateu.edu**), um den Aufwand bei der Eingabe zu verringern. Ihr Systemadministrator kann Ihnen sagen, ob der Dateibereich Ihrer Zelle auf diese Weise verkürzte Namen verwendet. Der Rest des Pfadnamens hängt davon ab, wie der Administrator der Zelle deren Dateibereich strukturiert hat.

Um auf Verzeichnisse und Dateien in AFS zuzugreifen, müssen Sie sowohl den korrekten Pfadnamen angeben als auch die erforderlichen Berechtigungen für die ACL besitzen, die das Verzeichnis und die Dateien darin schützt.

Beispiel: Anzeigen des Inhalts eines Verzeichnisses eines anderen Benutzers

Der Benutzer **terry** möchte nach einer Datei suchen, die dem anderen Benutzer **pat** gehört. Er gibt den Befehl **ls** mit dem entsprechenden Pfadnamen ein.

```
% ls /afs/abc.com/usr/pat/public
doc/                    directions/
guide/                  jokes/
library/
```

Zugreifen auf fremde Zellen

Sie können auf Dateien nicht nur in Ihrer eigenen Zelle zugreifen, sondern in jeder AFS-Zelle, die Sie über das Netzwerk erreichen können, ungeachtet des geografischen Standortes. Es gibt zwei zusätzliche Voraussetzungen:

- Die Liste fremder Zelle Ihres Cache Managers muß die Zelle, auf die Sie zugreifen möchten, enthalten. Nur der lokale Superuser **root** kann diese Zellenliste editieren, aber jeder kann sie sich anzeigen lassen. Siehe „Festlegen des Zugriffs auf fremde Zellen" auf Seite 30.
- Die ACL für das Verzeichnis, das die Datei beherbergt, und für jedes Elternverzeichnis im Pfadnamen muß Ihnen die notwendigen Berechtigungen erteilen. Der einfachste Weg für den Eigner des Verzeichnisses, die Berechtigungen auf fremde Benutzer zu erweitern, ist es, für die Gruppe **system:anyuser** in der ACL einen Eintrag unterzubringen.

  Die Alternative besteht darin, daß der fremde Administrator der Zelle für Sie ein Konto erstellt und Sie im Grunde damit zu einem lokalen Benutzer in der Zelle macht. Der Eigner des Verzeichnisses erstellt für Sie einen ACL-Eintrag wie für jeden anderen lokalen Benutzer. Um sich in der fremden Zelle zu authentifizieren, geben Sie den Befehl **klog** mit dem Argument **-cell** ein.

Eine weitere Beschreibung zum Schutz von Verzeichnissen und Dateien finden Sie in „Kapitel 4. Zugriffsschutz für Verzeichnisse und Dateien" auf Seite 33.

Ändern Ihres Kennworts

In Zellen, die ein für AFS modifiziertes Anmeldedienstprogramm verwenden, ist das Kennwort sowohl für das Anmelden als auch für das Authentifizieren bei AFS dasselbe. In diesem Fall verwenden Sie einen einzigen Befehl, **kpasswd**, um das Kennwort zu ändern.

Wenn Ihre Maschine über kein für AFS modifiziertes Anmeldedienstprogramm verfügt, gibt es für das Anmelden im lokalen Dateisystem und das Authentifizieren bei AFS getrennte Kennwörter: (Die zwei Kennwörter können nach Ihrem Ermessen gleich sein oder verschieden.) In diesem Fall verwenden Sie den Befehl **kpasswd**, um Ihr AFS-Kennwort zu ändern, und den UNIX-Befehl **passwd**, um Ihr UNIX-Kennwort zu ändern.

Ihr Systemadministrator kann die Sicherheit in der Zelle verbessern, indem er mehrere Funktionen zur Auswahl Ihres Kennworts konfiguriert. Denken Sie daran, wenn Sie den Befehl **kpasswd** eingeben:

- Zeitliche Begrenzung für die Gültigkeit Ihres Kennworts. Dies verbessert die Sicherheit Ihrer Zelle durch die zeitliche Begrenzung von Versuchen nicht autorisierter Benutzer, Ihr Kennwort zu erraten. Ihr Systemadministrator sollte Ihnen mitteilen, wann Ihr Kennwort abläuft, damit Sie es rechtzeitig ändern können. Der Administrator kann das für AFS modifizierte

Anmeldedienstprogramm so konfigurieren, daß diese Informationen jedesmal automatisch angezeigt werden, wenn Sie sich anmelden. Sie können auch den Befehl **kas examine** verwenden, um das Ablaufdatum des Kennworts anzuzeigen, wie in „So lassen Sie sich Ablaufdatum und Wiederverwendungsmaßnahme des Kennworts anzeigen" beschrieben.

Sie können zwar Ihr Kennwort vor dem Ablaufdatum ändern, Ihr Systemadministrator kann jedoch eine Mindestzeitspanne zwischen zwei Kennwortänderungen festlegen. Die folgende Nachricht zeigt an, daß diese Mindestzeitspanne noch nicht abgelaufen ist.

```
kpasswd: password was not changed because you changed it too
recently; see your system administrator
```

- Durchsetzen von Qualitätsstandards für Kennwörter wie Mindestlänge oder Einschluß von nichtalphabetischen Zeichen. Der Administrator sollte Sie über solche Anforderungen in Kenntnis setzen, damit Sie bei der Auswahl nicht akzeptabler Kennwörter nicht unnötig Zeit verschwenden.
- Zurückweisen eines Kennworts, das den letzten 20 von Ihnen verwendeten Kennwörtern zu ähnlich ist. Sie können den Befehl **kas examine** verwenden, um zu überprüfen, ob diese Maßnahme auf Sie zutrifft, wie in „So lassen Sie sich Ablaufdatum und Wiederverwendungsmaßnahme des Kennworts anzeigen" beschrieben. Die folgende Nachricht zeigt an, daß das von Ihnen gewählte Kennwort einem vorherigen Kennwort zu ähnlich ist.

  ```
  kpasswd: Password was not changed because it seems like a reused password
  ```

So lassen Sie sich Ablaufdatum und Wiederverwendungsmaßnahme des Kennworts anzeigen

Geben Sie den Befehl **kas examine** ein, um sich Ablaufdatum und Wiederverwendungsmaßnahme Ihres Kennworts anzeigen zu lassen. Sie können jedoch nur Ihr eigenes Konto überprüfen. Die dritte Zeile der Ausgabe enthält das Ablaufdatum Ihres Kennworts. Die letzte Zeile enthält die für Sie zutreffende Wiederverwendungsmaßnahme des Kennworts.

```
   % kas examine Ihr_Benutzername
Password for Ihr_Benutzername: Ihr_AFS_Kennwort
```

Das folgende Beispiel stellt die Ausgabe für den Benutzer **pat** dar.

```
   User data for pat
key (15) cksum is 3414844392, last cpw: Thu Oct 21 16:05:44 1999
password will expire: Fri Nov 26 20:44:36 1999
9 consecutive unsuccessful authentications are permitted.
The lock time for this user is 25.5 minutes.
User is not locked.
entry never expires. Max ticket lifetime 100.00 hours.
last mod on Wed Aug 18 08:22:29 1999 by admin
don't permit password reuse
```

So ändern Sie Ihr AFS-Kennwort

Verwenden Sie den Befehl **kpasswd**, der Sie zur Eingabe des alten und des neuen Kennworts und zur Bestätigung des neuen Kennworts auffordert. Die Kennwörter werden nicht sichtbar auf dem Bildschirm wiedergegeben.

```
   % kpasswd
Old password: Aktuelles_Kennwort
New password (RETURN to abort): Neues_Kennwort
Retype new password: Neues_Kennwort
```

So ändern Sie Ihr UNIX-Kennwort

Verwenden Sie den UNIX-Befehl **passwd**, der Sie zur Eingabe des alten und des neuen Kennworts und zur Bestätigung des neuen Kennworts auffordert. Die Kennwörter werden nicht sichtbar auf dem Bildschirm widergegeben. Auf vielen Maschinen befindet sich **passwd** im Verzeichnis **/bin**, und Sie müssen möglicherweise den vollständigen Pfadnamen eingeben.

```
   % passwd
Changing password for username.
Old password: Aktuelles_Kennwort
New password: Neues_Kennwort
Retype new passwd: Neues_Kennwort
```

Kapitel 3. Anzeigen von Informationen zu AFS

In diesem Kapitel wird beschrieben, wie Informationen angezeigt werden, die zur effektiveren Verwendung von AFS dienen. Das Kapitel enthält folgende Abschnitte:

„Anzeigen der Quote eines Volumes"

„Suchen von Dateien und Verzeichnissen" auf Seite 28.

„Prüfen des Status von Server-Maschinen" auf Seite 29

„Festlegen des Zugriffs auf fremde Zellen" auf Seite 30

„Anzeigen der Rangordnung von Servern" auf Seite 31

Anzeigen der Quote eines Volumes

Üblicherweise werden die Dateien im Ausgangsverzeichnis gemeinsam auf einem einzigen Volume gespeichert. (Informationen zu Volumes enthält der Abschnitt „Volumes und Mount-Punkte" auf Seite 3.) Damit der verfügbare Plattenspeicherplatz einer Zelle möglichst optimal zugeordnet wird, geben die Systemadministratoren für jedes Volume eine Größenbegrenzung, die sogenannte *Quote*, an. Sie können nicht mehr Daten auf einem Volume speichern, als es seine Quote es zuläßt. Wenn bei einem Volume die angegebene Quote nahezu erreicht ist, können Sie manchmal keine Änderungen speichern, die Sie an Dateien vorgenommen haben, die auf dem Volume gespeichert sind.

Die Menge des verfügbaren Speicherplatzes auf der Partition, auf der sich das Volume befindet, begrenzt auch die Größe, auf die das Volume anwachsen kann. Wenn die Plattenpartition voll ist, kann es sein, daß Sie keine Änderungen mehr an einer Datei speichern können, selbst wenn bei dem Volume die angegebene Quote noch nicht erreicht ist.

Prüfen Sie die Quote des Ausgangs-Volumes regelmäßig, um sicherzustellen, daß ausreichend Speicherplatz vorhanden ist. Wenn Sie Probleme beim Sichern einer Datei feststellen, überprüfen Sie die Quote des Volumes, auf dem die Datei gespeichert wird. Verwenden Sie die folgenden Befehle, um die Quote des Volumes anzuzeigen.

- Mit dem Befehl **fs quota** wird der Prozentsatz an verwendeter Quote des Volumes aufgelistet.
- Sowohl mit dem Befehl **fs listquota** als auch mit dem Befehl **fs examine** werden der Name des Volumes, die maximale Größe (Quote) und die aktuelle Größe aufgelistet. Mit diesen Befehlen werden außerdem die folgenden Informationen emittiert.

© Copyright IBM Corp. 1989, 2000

– Mit dem Befehl **fs listquota** wird der verwendete Prozentsatz sowohl des Volumes als auch der Partition aufgelistet.
– Mit dem Befehl **fs examine** werden die Größe der Partition, die Menge des aktuell verwendeten Speicherplatzes und alle Nachrichten aufgelistet, die dem Volume zugeordnet sind.

Anzeigen des Prozentsatzes der verwendeten Quote

Führen Sie den Befehl **fs quota** aus, um den Prozentsatz der Quote anzuzeigen, die derzeit für das Volume verwendet wird, das ein bestimmtes Verzeichnis oder eine bestimmte Datei enthält.

```
% fs quota [<Verzeichnis-/Dateipfad>+]
```

Dabei steht *Pfad d. Verzeichnisses/Datei* für den Pfadnamen einer Datei oder eines Verzeichnisses auf jedem Volume, für das Quoteninformationen angezeigt werden sollen. Wenn kein Pfadname angegeben wird, werden Quoteninformationen für das Volume angegeben, das das aktuelle Arbeitsverzeichnis enthält.

Beispiel: Anzeigen des verwendeten Prozentsatzes der Quote

Im folgenden Beispiel wird der verwendete Prozentsatz der Quote für die Volumes angezeigt, die zwei Benutzerausgangsverzeichnisse in der Zelle der Firma ABC Corporation enthalten.

```
% cd /afs/abc.com/usr
% fs quota terry pat
34% of quota used.
85% of quota used.
```

Anzeigen der Quote und weiterer Informationen zu einem Volume

Führen Sie den Befehl **fs listquota** aus, um die folgenden Informationen anzuzeigen:

- Den Namen des Volumes, auf dem sich die angegebene Datei oder das Verzeichnis befindet.
- Die Quote, ausgedrückt als Anzahl von Kilobyte (1024 Kilobyte sind 1 Megabyte).
- Die aktuelle Größe des Volumes (die tatsächlich verwendete Anzahl Kilobyte).
- Den Prozentsatz der verwendeten Quote.
- Den Prozentsatz des verwendeten Speicherbereichs auf der Plattenpartition, auf der sich das Volume befindet.

Die Befehlssyntax ist wie folgt:

```
% fs listquota [<Verzeichnis-/Dateipfad>+]
```

Dabei steht *Pfad d. Verzeichnisses/Datei* für den Pfadnamen einer Datei oder eines Verzeichnisses auf jedem Volume, für das Quoteninformationen angege-

ben werden. Wenn kein Pfadname angegeben wird, gibt die Ausgabe Quoteninformationen für das Volume an, welche das aktuelle Arbeitsverzeichnis enthält.

Beispiel: Anzeigen der Quote und anderer Informationen zu einem Volume

Im folgenden Beispiel werden die Quoteninformationen zu einem Volume angezeigt, auf dem sich das Ausgangsverzeichnis des Benutzers **terry** befindet.

```
% fs listquota ~terry
Volume Name     Quota    Used    % Used   Partition
user.terry      10000    3400       34%         86%
```

Anzeigen der Quote und weiterer Informationen zu einem Volume und einer Partition

Führen Sie den Befehl **fs examine** aus, um die folgenden Informationen zu einem Volume und der Partition, auf der sich das Volume befindet, anzuzeigen:

- Die ID-Nummer des Volumes (in der Ausgabe als `vid` abgekürzt).
- Den Namen des Volumes.
- Die Quote des Volumes und die aktuelle Größe in Kilobyte.
- Die Anzahl der Kilobyteblöcke, die auf der Plattenpartition zur Verfügung stehen, auf der sich das Volume befindet, und die Gesamtgröße dieser Partition.
- Gegebenenfalls eine *Offline-Nachricht*, die dem Volume zugeordnet ist, wie von einem Systemadministrator festgelegt.

Die Befehlssyntax ist wie folgt:

```
% fs examine [<Verzeichnis-/Dateipfad>+]
```

Dabei wird mit *Pfad d. Verzeichnisses/Datei* der Pfadname einer Datei oder eines Verzeichnisses auf jedem Volume angegeben, für das Quoteninformationen angezeigt werden sollen. Wenn kein Pfadname angegeben wird, gibt die Ausgabe Quoteninformationen für das Volume an, auf dem sich das aktuelle Arbeitsverzeichnis befindet.

Beispiel: Anzeigen der Quote und weiterer Informationen zu einem Volume und einer Partition

Im folgenden Beispiel werden Quoten- und weitere Informationen zu dem Volume angezeigt, auf dem sich das aktuelle Arbeitsverzeichnis befindet.

```
% fs examine
Volume status for vid = 536871122 named user.terry
Current disk quota is 10000
Current blocks used are 5745
The partition has 1593 blocks available out of 99162
```

Suchen von Dateien und Verzeichnissen

Normalerweise brauchen Sie nicht zu wissen, auf welcher Datei-Server-Maschine das Volume gespeichert ist, der eine Datei oder ein Verzeichnis enthält. Wenn der Pfadname für eine Datei angegeben ist, greift der Cache Manager der Client-Maschine automatisch auf die entsprechende Server-Maschine zu.

Wenn der Zugriff auf eine Datei nicht möglich ist, kann es jedoch hilfreich sein, zu wissen, auf welcher Datei-Server-Maschine sich die Datei befindet. Sie können dann prüfen, ob der File Server-Prozeß und die entsprechende Maschine korrekt arbeiten (siehe „Prüfen des Status von Server-Maschinen” auf Seite 29). Außerdem können Sie, wenn Ausfallzeiten für eine Maschine eingeplant sind, erfahren, ob es wahrscheinlich ist, daß ein Ausfall dazu führt, daß auf bestimmte Dateien nicht zugegriffen werden kann.

Anzeigen der Position einer Datei oder eines Verzeichnisses

Führen Sie den Befehl **fs whereis** aus, um die Datei-Server-Maschine anzuzeigen, auf der eine Datei oder ein Verzeichnis gespeichert ist.

```
% fs whereis [<Verzeichnis-/Dateipfad>+]
```

Dabei wird mit *Pfad d. Verzeichnisses/Datei* der Pfadname jeder Datei oder jedes Verzeichnisses angegeben, für die Informationen zur Position angefordert werden. Wenn Sie keinen Pfadnamen angeben, gibt die Ausgabe die Maschine an, auf der sich das Volume befindet, welches das aktuelle Arbeitsverzeichnis enthält.

Wenn in der Ausgabe mehrere Maschinen angegeben werden, existiert an jedem Standort eine Kopie des Volumes (das Volume wird *repliziert*). Systemadministratoren können angeben, daß Volumes repliziert werden sollen, die Informationen enthalten, welche von vielen Personen benötigt werden. Für eine Replikation spricht zum einen der Lastausgleich und zum anderen die Möglichkeit, Informationen zur Verfügung stellen zu können, selbst wenn es auf der Maschine, auf der sich das Volume befindet, zu einem Ausfall kommt.

Beispiel: Anzeigen der Verzeichnisposition

Im folgenden Beispiel werden die Namen der Server-Maschinen angezeigt, auf denen sich die Volumes für die Benutzer **terry** und **pat** befinden.

```
% cd /afs/abc.com/usr
% fs whereis terry pat
File /afs/abc.com/usr/terry is on host fs2.abc.com
File /afs/abc.com/usr/pat is on host fs3.abc.com
```

Prüfen des Status von Server-Maschinen

Manchmal kann auf eine oder mehrere Server-Maschinen in einer Zelle aufgrund von Hardware-Problemen, Software-Problemen oder Routine-Wartungsarbeiten nicht zugegriffen werden. Während des Ausfalls können Sie nicht auf Dateien zugreifen, die auf solchen Maschinen gespeichert sind, oder Änderungen speichern, die an Dateien vorgenommen wurden, die auf diesen Maschinen gespeichert sind. (Der Cache Manager verfügt möglicherweise über lokal gespeicherte Kopien dieser Dateien, mit denen Sie noch arbeiten können.)

Um den Status von Server-Maschinen zu überprüfen, verwenden Sie den Befehl **fs checkservers**. Wenn eine Server-Maschine über mehr als eine Netzschnittstellenadresse verfügt (wenn sie *mehrfach vernetzt* (multihomed) ist), sendet der Cache Manager die Nachricht zur Statusprüfung an alle Schnittstellen der Maschine. Wenn mindestens eine der Schnittstellen des Servers antwortet, gibt die Ausgabe des Befehls an, daß auf die Maschine zugegriffen werden kann. Wenn keine der Schnittstellen eine Antwort gibt, gibt die Ausgabe an, daß nicht auf die Maschine zugegriffen werden kann. Eine der Schnittstellen wird jedoch mit angezeigt (in der Regel die mit dem höchsten Rang; siehe „Anzeigen der Rangordnung von Servern” auf Seite 31).

Um den Status verschiedener Gruppen von Server-Maschinen zu überprüfen, kombinieren Sie die Optionen des Befehls **fs checkservers** wie folgt:

- Wenn nur Datei-Server-Maschinen überprüft werden sollen, die sich in der lokalen Zelle befinden, geben Sie keine Optionen an.
- Wenn nur Datei-Server-Maschinen überprüft werden sollen, die sich in einer bestimmten fremden Zelle befinden, geben Sie das Argument **-cell** an.
- Wenn jede Datei-Server-Maschine überprüft werden soll, zu der der Cache Manager in einer beliebigen Zelle Kontakt aufgenommen hatte, geben Sie die Markierung **-all** an.

Es kann einige Minuten dauern, bis die Eingabeaufforderung der Befehls-Shell wieder emittiert wird, da der Befehls-Interpreter für **fs**-Befehle die als Zeitlimit angegebene Zeitspanne abwartet, bevor die Schlußfolgerung gezogen wird, daß der Zugriff auf eine Maschine, die nicht antwortet, tatsächlich nicht möglich ist. Wenn die Eingabeaufforderung der Befehls-Shell sofort emittiert werden soll, fügen Sie das Et-Zeichen (**&**) hinzu. Dadurch wird der Befehl **fs checkservers** im Hintergrund ausgeführt.

Überprüfen des Status von Datei-Server-Maschinen

Führen Sie den Befehl **fs checkservers** aus, um den Status von Datei-Server-Maschinen zu überprüfen.

```
% fs checkservers [-cell <zu überprüfende Zelle>] [-all] [&]
```

Dabei gilt folgendes:

-cell gibt jede Zelle an, für die der Status der Server-Maschine überprüft werden soll. Dieses Argument und die Markierung **-all** dürfen nicht kombiniert werden.

-all prüft den Status aller Server-Maschinen. Diese Markierung und das Argument **-cell** dürfen nicht kombiniert werden.

Wenn die folgende Nachricht emittiert wird, bedeutet dies, daß alle Server-Maschinen auf die Nachricht des Cache Managers zur Statusprüfung antworteten:

```
All servers are running.
```

Andernfalls werden mit einer Nachricht, die der folgenden ähnlich ist, die Maschinen aufgelistet, auf die nicht zugegriffen werden kann:

```
These servers unavailable due to network or server problems: Liste der Maschinen.
```

Beispiel: Überprüfen des Status von Server-Maschinen

Im folgenden Beispiel wird der Status jeder Datei-Server-Maschine überprüft, zu der der Cache Manager in einer beliebigen Zelle Kontakt aufgenommen hat. Zwei Maschinen antworten nicht.

```
% fs checkservers -all &
%These servers unavailable due to network or server problems:
    fs1.abc.com server7.stateu.edu.
```

Festlegen des Zugriffs auf fremde Zellen

Der Cache Manager verwaltet eine Liste fremder Zellen, von denen er weiß, wie er auf sie zugreifen kann. Eine Zelle muß in der Liste angezeigt werden, damit Sie auf deren AFS-Dateibereich zugreifen können. (Zusätzlich dazu muß Ihnen die ACL in jedem Verzeichnis, das im Pfadnamen für die Datei angegeben ist, die erforderlichen Berechtigungen erteilen, und der Systemadministrator muß die Zelle im lokalen AFS-Dateibereich anhängen. Üblicherweise wird der AFS-Dateibereich direkt unter dem Verzeichnis **/afs** angehängt.)

Anzeigen fremder Zellen

Führen Sie den Befehl **fs listcells** aus, um die Zellen anzuzeigen, auf die Sie von einer Client-Maschine aus zugreifen können. Es kann einige Minuten dauern, bis die Eingabeaufforderung der Befehls-Shell wieder emittiert wird. Der Cache Manager speichert die Maschinen als IP-Adressen, setzt die Adressen aber in Namen um, bevor sie angezeigt werden. Wenn die Eingabeaufforderung der Befehls-Shell sofort emittiert werden soll, fügen Sie das Et-Zeichen (**&**) hinzu. Dadurch wird der Befehl **fs listcells** im Hintergrund ausgeführt. Beispiel:

```
% fs listcells &
 %Cell abc.com  on hosts
     db1.abc.com
     db2.abc.com
```

```
     db3.abc.com
Cell test.abc.com on hosts
     test4.abc.com.
Cell stateu.edu on hosts
     sv5.stateu.edu.
     sv2.stateu.edu.
     sv11.stateu.edu.
Cell def.com on hosts
     serverA.def.com
```

Anzeigen der Rangordnung von Servern

Der Cache Manager speichert eine Liste mit der Rangordnung von Datei-Server-Maschinen. Wenn der Cache Manager auf eine Datei oder ein Verzeichnis zugreifen muß, vergleicht er die Rangwerte der Datei-Server-Maschinen, auf denen sich das betroffene Volume befindet. Zuerst wird versucht, auf das Volume zuzugreifen, der sich auf der Maschine mit dem höchsten Rang befindet. (Wenn eine Datei-Server-Maschine mehrfach vernetzt ist, d.h. über mehrere Netzschnittstellen verfügt, ordnet der Cache Manager jeder Schnittstelle einen separaten Rang zu.)

Der Cache Manager ordnet der Schnittstelle einer Datei-Server-Maschine einen Standardrang zu, indem er die eigene IP-Adresse mit der IP-Adresse der Schnittstelle vergleicht. Er ordnet Schnittstellen, die sich in seinem eigenen Teilnetz oder Netzwerk befinden, einen höheren Rang zu als Schnittstellen in anderen Netzwerken. Daher beeinflussen die Rangwerte den Cache Manager dahingehend, Dateien aus den Datei-Server-Maschinen abzurufen, die sich bezüglich des Netzabstands nahe bei ihm befinden. Dadurch wird der Datenaustausch im Netz reduziert und der Cache Manager dabei unterstützt, Daten an Anwendungen schneller zu liefern.

Der Cache Manager speichert jeden Rang als Wertepaar bestehend aus IP-Adresse der Schnittstelle einer Datei-Server-Maschine und einer den Rang ausdrückenden ganzen Zahl zwischen **0** und **65.534**. Eine niedrigere Zahl repräsentiert einen höheren Rang. Um die Werte der Server-Rangordnung auf der lokalen Client-Maschine anzuzeigen, führen Sie den Befehl **fs getserverprefs** aus.

Der Cache Manager speichert eine separate, aber ähnliche Menge an Rangwerten für VL-Server (VL = Volume Location), die dem Cache Manager Informationen zur Position von Volumes zukommen lassen, auf denen sich Dateien und Verzeichnisse befinden. Zum Anzeigen dieser Rangwerte fügen Sie dem Befehl **fs getserverprefs** die Markierung **-vlservers** hinzu.

Wenn es so aussieht, als führten die Standardrangwerte nicht zur besten Leistung, kann der Systemadministrator eine Änderung an ihnen vornehmen. Befragen Sie gegebenenfalls den Systemadministrator zu den Rangwerten.

Anzeigen von Werten für die Server-Rangordnung

Führen Sie den Befehl **fs getserverprefs** aus, um die Rangwerte der Datei-Server-Maschinen anzuzeigen, die vom Cache Manager der lokalen Maschine verwendet werden. Zum Anzeigen der VL-Server-Rangwerte fügen Sie dem Befehl die Markierung **-vlservers** hinzu. Standardmäßig setzt der Cache Manager die IP-Adresse jeder Schnittstelle vor dem Anzeigen in einen Host-Namen um. Um diese Umsetzung zu umgehen und IP-Adressen anzuzeigen, fügen Sie die Markierung **-numeric** hinzu. Dies kann die Ausgabe des Befehls erheblich beschleunigen.

```
% fs getserverprefs [-numeric] [-vlservers]
```

Im folgenden Beispiel werden die Rangwerte der Datei-Server-Maschinen für eine Client-Maschine in der Zelle **abc.com** angezeigt. Die Rangwerte der Datei-Server-Maschinen in dieser Zelle sind niedriger als die Rangwerte der Datei-Server-Maschinen in der fremden Zelle **def.com**. Da die Markierung **-numeric** nicht verwendet wird, zeigt die Ausgabe Host-Namen an. Die Ausgabe der IP-Adresse für zwei Maschinen bedeutet, daß die Umsetzung nicht möglich war.

```
% fs getserverprefs
fs2.abc.com           20007
fs3.abc.com           30002
fs1.abc.com           20011
fs4.abc.com           30010
server1.def.com       40002
192.12.105.34         40000
server6.def.com       40012
192.12.105.37         40005
```

Kapitel 4. Zugriffsschutz für Verzeichnisse und Dateien

In diesem Kapitel wird erläutert, wie AFS-Dateien und -Verzeichnisse vor unbefugtem Zugriff geschützt werden, indem Berechtigungen in einer Zugriffssteuerungsliste definiert werden.

Zugriffssteuerungslisten

AFS weitet das Standard-UNIX-Schema für die Steuerung des Zugriffs auf Dateien und Verzeichnisse aus und verbessert es. Anstelle der Verwendung von Modusbits zum Definieren der Zugriffsberechtigungen für einzelne Dateien, wie bei UNIX, wird bei AFS mit jedem Verzeichnis eine *Zugriffssteuerungsliste* (*ACL, Access Control List*) gespeichert. In der ACL ist definiert, welche Benutzer und Gruppen auf das Verzeichnis und die darin enthaltenen Dateien zugreifen können und welche Arten von Zugriff möglich sind. In einer ACL können bis zu 20 Einträge gespeichert werden. Dabei ist jeder Eintrag eine Kombination aus einem Benutzer oder einer Gruppe und einer Menge von Berechtigungen. In AFS sind sieben Berechtigungen definiert, nicht nur die drei, die in UNIX verwendet werden.

Eine weitere Verbesserung im Vergleich zu dem Standardzugriffsschutzschema unter UNIX ist, daß Benutzer ihre eigenen *Gruppen* für den Zugriffsschutz definieren können und diese Gruppen dann in ACLs stellen können, als wären diese einzelne Benutzer. Eine Gruppe kann sowohl Benutzer als auch Maschinen enthalten. Jeder Benutzer, der zu einer Gruppe gehört, übernimmt alle Berechtigungen, die der Gruppe in der ACL erteilt werden. Gleichermaßen übernehmen alle Benutzer, die an einer Maschine angemeldet sind, die zu einer Gruppe gehört, alle Berechtigungen, die der Gruppe erteilt werden. Sie können Gruppen erstellen, die dann in ACLs gestellt werden, und können auch Gruppen verwenden, die andere Benutzer erstellt haben. Weitere Informationen zum Erstellen von Gruppen enthält „Kapitel 5. Verwendung von Gruppen” auf Seite 53.

Zusätzlich dazu sind in AFS zwei Systemgruppen definiert: **system:anyuser** und **system:authuser**. Indem Sie diese Gruppen in ACLs stellen, können Sie einer großen Anzahl Benutzer gleichzeitig den Zugriff erteilen. Weitere Informationen hierzu erhalten Sie unter „Verwenden von Systemverwaltungsgruppen in ACLs” auf Seite 38.

AFS verwendet zwar ACLs für den Zugriffsschutz für Dateien und Verzeichnisse, AFS verwendet jedoch auch in beschränktem Umfang UNIX-Modusbits. Weitere Informationen hierzu erhalten Sie unter „Verwendung der UNIX-Modusbits durch AFS” auf Seite 50.

© Copyright IBM Corp. 1989, 2000

Zugriffssteuerung auf Verzeichnisebene

Wie bereits erläutert, ordnet AFS jedem Verzeichnis eine ACL zu, die für alle in dem Verzeichnis gespeicherten Dateien gilt. Für Dateien gelten keine verschiedenen ACLs. Die Definition des Zugriffs auf der Verzeichnisebene hat verschiedene Folgen:

- Die in einer ACL eines Verzeichnisses definierten Berechtigungen gelten für alle im Verzeichnis enthaltenen Dateien. Wenn eine Datei in ein anderes Verzeichnis verschoben wird, werden die für die Datei geltenden Berechtigungen durch jene Berechtigungen ersetzt, die in der ACL des neuen Verzeichnisses definiert sind. Wenn die ACL eines Verzeichnisses geändert wird, ändert sich der Zugriffsschutz für alle in dem Verzeichnis enthaltenen Dateien.
- Wenn Sie ein Unterverzeichnis erstellen, übernimmt dieses Verzeichnis die aktuelle ACL des Elternverzeichnisses. Anschließend können Sie die ACL des Unterverzeichnisses so definieren, daß sie von der ACL des Elternverzeichnisses abweicht. Definieren Sie die ACL für das Elternverzeichnisses jedoch nicht mit mehr Einschränkungen als die ACL des Unterverzeichnisses. In diesem Fall kann Benutzern der Zugriff auf das Unterverzeichnis verweigert werden, selbst wenn sie über die erforderlichen Berechtigungen verfügen, die in der ACL des Unterverzeichnisses festgelegt sind. Ein Benutzer muß insbesondere über die **l** (**lookup**)-Berechtigung (siehe „AFS-ACL-Berechtigungen”) für das Elternverzeichnis verfügen, um auf dessen Unterverzeichnisse zugreifen zu können.

Im allgemeinen ist es sinnvoll, wenn Sie einen möglichst freien Zugriff auf Ihr Ausgangsverzeichnis erteilen. Wenn für bestimmte Dateien ein höherer Zugriffsschutz gelten soll, stellen Sie diese in Unterverzeichnisse, für die ACLs mit mehr Einschränkungen gelten.

AFS-ACL-Berechtigungen

Es stehen sieben Standardberechtigungen für ACLs in AFS zur Verfügung. Funktionstechnisch sind diese in zwei Gruppen einzuteilen: eine Gruppe, die sich auf das Verzeichnis selbst bezieht, und die andere, die sich auf die Dateien bezieht.

Vier Berechtigungen für das Verzeichnis

Die vier Berechtigungen in dieser Gruppe beziehen sich auf das Verzeichnis selbst. Zum Beispiel wird mit der **i** (**insert**)-Berechtigung die Erstellung einer neuen Datei oder eines neuen Unterverzeichnisses gesteuert, und nicht das Hinzufügen von Daten in eine Datei.

l (lookup)-Berechtigung

Die Funktionsweise dieser Berechtigung ist vergleichbar mit einem Pförtner, der den Zugriff auf das Verzeichnis und die darin enthaltenen Dateien freigibt oder nicht. Ein Benutzer muß über diese Berechti-

gung verfügen, um mit anderen Berechtigungen zu arbeiten. Insbesondere muß ein Benutzer über diese Berechtigung verfügen, um auf Daten in den Unterverzeichnissen des Verzeichnisses zuzugreifen.

Mit dieser Berechtigung kann ein Benutzer einen der folgenden Befehle ausführen:

- Befehl **ls** zum Auflisten der Namen der Dateien und Unterverzeichnisse im Verzeichnis
- Befehl **ls -ld** zum Abrufen vollständiger Statusinformationen für das Verzeichniselement selbst
- Befehl **fs listacl** zum Prüfen der Verzeichnis-ACL

Mit dieser Berechtigung kann ein Benutzer nicht den Inhalt einer Datei im Verzeichnis lesen oder den Befehl **ls -l** oder **fs listacl** mit einem Dateinamen als Argument ausführen. Für diese Operationen ist die **r** (**read**)-Berechtigung erforderlich, die unter „Drei Berechtigungen für die Datei" auf Seite 36 beschrieben ist.

Gleichermaßen ermöglicht diese Berechtigung einem Benutzer nicht, die Befehle **ls**, **ls -l**, **ls -ld** oder **fs listacl** für ein Unterverzeichnis des Verzeichnisses auszuführen. Für diese Operationen ist die **l**-Berechtigung in der ACL des Unterverzeichnisses selbst erforderlich.

i (insert)-Berechtigung

Mit dieser Berechtigung kann ein Benutzer dem Verzeichnis neue Dateien hinzufügen - entweder durch Erstellen oder durch Kopieren - und neue Unterverzeichnisse erstellen. Die Berechtigung gilt nicht für Unterverzeichnisse. Diese sind durch ihre eigenen ACLs geschützt.

d (delete)-Berechtigung

Mit dieser Berechtigung kann ein Benutzer Dateien und Unterverzeichnisse aus dem Verzeichnis entfernen oder sie in andere Verzeichnisse verschieben (unter der Voraussetzung, daß der Benutzer über die **i**-Berechtigung in der ACL der anderen Verzeichnisse verfügt).

a (administer)-Berechtigung

Mit dieser Berechtigung kann ein Benutzer die ACL eines Verzeichnisses ändern: Mitglieder der Gruppe **system:administrators** verfügen implizit über diese Berechtigung für jedes Verzeichnis (das heißt, selbst wenn diese Gruppe nicht in der ACL aufgeführt wird). Gleichermaßen verfügt der Eigner eines Verzeichnisses implizit über diese Berechtigung für seine ACL und für alle untergeordneten Verzeichnisse.

Drei Berechtigungen für die Datei

Die drei Berechtigungen in dieser Gruppe beziehen sich auf Dateien in einem Verzeichnis, und nicht auf das Verzeichnis selbst oder dessen Unterverzeichnisse.

r (read)-Berechtigung
Mit dieser Berechtigung kann ein Benutzer den Inhalt von Dateien im Verzeichnis lesen und den Befehl **ls -l** ausführen, um die Dateielemente anzugeben.

w (write)-Berechtigung
Mit dieser Berechtigung kann ein Benutzer den Inhalt von Dateien im Verzeichnis ändern und den Befehl **chmod** ausführen, um deren UNIX-Modusbits zu ändern.

k (lock)-Berechtigung
Mit dieser Berechtigung kann ein Benutzer Programme ausführen, welche Systemaufrufe durchführen, mit denen Dateien im Verzeichnis gesperrt werden.

Acht zusätzliche Berechtigungen

AFS stellt acht zusätzliche Berechtigungen zur Verfügung, die keine definierte Bedeutung haben. Diese werden durch die Großbuchstaben **A**, **B**, **C**, **D**, **E**, **F**, **G** und **H** angegeben.

Der Systemadministrator kann Anwendungsprogramme schreiben, die einer oder mehreren dieser Berechtigungen eine Bedeutung zuweisen. Er kann diese Berechtigungen dann in ACLs stellen, um den Dateienzugriff durch diese Programme zu steuern. Mit den Befehlen **fs listacl** und **fs setacl** können Sie die zusätzlichen Berechtigungen anzeigen und in ACLs definieren, wie dies bereits für die sieben Standardberechtigungen gilt.

Kurzformen für Mengen an Berechtigungen

Sie können die sieben Berechtigungen in einem ACL-Eintrag beliebig kombinieren. Bestimmte Kombinationen sind jedoch vorteilhafter als andere. Vier der gängigen Kombinationen verfügen über entsprechende Kurzformen. Wenn der Befehl **fs setacl** zum Definieren der ACL-Einträge verwendet wird, können Sie entweder einen oder mehrere einzelne Buchstaben angeben, die die Berechtigungen darstellen, oder eine der folgenden Kurzformen:

all Steht für alle sieben Standardberechtigungen (**rlidwka**).

none Entfernt den Eintrag aus der ACL. Der Benutzer oder die Gruppe verfügen über keine Berechtigung mehr.

read Steht für die Berechtigungen **r** (**read**) und **l** (**lookup**).

write Steht für alle Berechtigungen außer **a** (**administer**): **rlidwk**.

Normale und negative Berechtigungen

ACLs ermöglichen es Ihnen, Zugriff auf ein Verzeichnis und die darin enthaltenen Dateien zu erteilen und zu verweigern. Zum Erteilen des Zugriffs verwenden Sie den Befehl **fs setacl**, um einen ACL-Eintrag zu erstellen, der einem Benutzer oder einer Gruppe eine Menge an Berechtigungen zuordnet (siehe die Beschreibung unter „Ändern einer ACL" auf Seite 42). Wenn Sie eine ACL mit dem Befehl **fs listacl** anzeigen (siehe die Beschreibung unter „Anzeigen einer ACL" auf Seite 40, werden solche Einträge unter der folgenden Überschrift angezeigt:

```
Normal rights
```

Es gibt zwei Möglichkeiten, den Zugriff zu verweigern:

1. Die empfohlene Methode besteht darin, einen Eintrag für den Benutzer oder die Gruppe aus der ACL zu entfernen oder die entsprechenden Berechtigungen aus einem Eintrag zu entfernen. Verwenden Sie den Befehl **fs setacl**, um einen vorhandenen Eintrag zu entfernen oder zu editieren. In den meisten Fällen ist diese Methode ausreichend dafür, bestimmte Arten von Zugriff oder den Zugriff bestimmter Benutzer zu unterbinden. Dabei müssen Sie darauf achten, daß die Berechtigungen, die für einen bestimmten Benutzer nicht gelten sollen, nicht Gruppen erteilt werden, zu denen dieser Benutzer gehört.
2. Die explizitere Methode, den Zugriff zu verweigern, besteht darin, einen Eintrag in den Abschnitt mit den *negativen Berechtigungen* einer ACL zu stellen, indem die Markierung **-negative** in den Befehl **fs setacl** integriert wird. Anweisungen hierzu sind unter „Hinzufügen, Entfernen oder Editieren negativer ACL-Berechtigungen" auf Seite 45 enthalten. Mit dem Befehl **fs listacl** wird der Abschnitt mit den negativen Berechtigungen in einer ACL unter der folgenden Überschrift angezeigt:

   ```
   Negative rights
   ```

   Wenn bestimmt wird, welche Art von Zugriff einem Benutzer erteilt wird, überprüft ein AFS zuerst alle Einträge im Abschnitt mit den normalen Berechtigungen der ACL. Er zieht dann davon alle dem Benutzer (oder den Gruppen, zu denen der Benutzer gehört,) zugeordneten Berechtigungen im Abschnitt mit den negativen Berechtigungen in der ACL ab. Negative Berechtigungen setzen also immer entsprechende normale Berechtigungen außer Kraft.

   Das Arbeiten mit negativen Berechtigungen kann etwas verwirrend sein, da negative Berechtigungen die normale Bedeutung des Befehls **fs setacl** umkehren. Insbesondere ist die Kombination der Kurzform **none** mit der Markierung **-negative** eine doppelte Negierung: Durch Entfernen eines Eintrags aus dem Abschnitt mit den negativen Berechtigungen in der ACL kann ein Benutzer wieder Berechtigungen über Einträge im Abschnitt mit

den normalen Berechtigungen erhalten. Durch die Kombination der Kurzform **all** mit der Markierung **-negative** werden alle Berechtigungen explizit verweigert.

Die Negierung durch einen Eintrag im Abschnitt mit den negativen Berechtigungen ist nicht wirksam, wenn diese verweigerten Berechtigungen der Gruppe **system:anyuser** durch einen Eintrag im Abschnitt mit den normalen Berechtigungen erteilt werden. In diesem Fall können Benutzer die Berechtigungen einfach dadurch erhalten, daß Sie mit dem Befehl **unlog** ihre Token löschen. AFS erkennt den Benutzer dann als Benutzer **anonymous**, der zu der Gruppe **system:anyuser** gehört, aber keine Übereinstimmung mit den Einträgen im Abschnitt mit den negativen Berechtigungen in der ACL aufweist.

Konfigurieren von DFS-ACLs

Wenn die verwendete Maschine so konfiguriert ist, daß der Zugriff auf einen DFS-Dateibereich einer DCE-Zelle über das AFS/DFS Migration Toolkit erfolgt, können Sie mit den AFS-Befehlen **fs listacl** und **fs setacl** die ACLs in DFS-Verzeichnissen und -Dateien, deren Eigner Sie sind, anzeigen und konfigurieren. DFS verwendet eine leicht abweichende Menge an Berechtigungen und eine andere Syntax für ACL-Einträge. Lesen Sie die entsprechenden Informationen in der DFS-Dokumentation, oder fragen Sie den Systemadministrator dazu.

Verwenden von Systemverwaltungsgruppen in ACLs

AFS definiert zwei *Systemverwaltungsgruppen*, die Zugriff auf eine große Anzahl von Benutzern gleichzeitig erteilen, wenn sie in die ACL gestellt werden. Sie können jedoch nicht die Zugehörigkeit zu diesen Gruppen beeinflussen. Gehen Sie daher sorgfältig vor, wenn Sie entscheiden, welche Berechtigungen diesen Gruppen erteilt werden sollen. (Sie können nur die Zugehörigkeit zu den Gruppen steuern, deren Eigner Sie sind; siehe „Kapitel 5. Verwendung von Gruppen” auf Seite 53.)

system:anyuser
: Enthält jeden beliebigen Benutzer, der auf den Dateibaum der Zelle zugreifen kann, einschließlich der Benutzer, die über Token in der lokalen Zelle verfügen, derjenigen, die sich an einer lokalen AFS-Client-Maschine angemeldet, aber keine Token erhalten haben (wie z.B. der lokale Superuser **root**), und der Benutzer, die von außerhalb der Zelle eine Verbindung zu einer lokalen Maschine hergestellt haben. Das Erstellen eines ACL-Eintrags für diese Gruppe ist die einzige Möglichkeit, den Zugriff auf AFS-Benutzer fremder Zellen zu erweitern, es sei denn, der Systemadministrator erstellt lokale Authentifizierungskonten für sie.

system:authuser
Enthält alle Benutzer, die über einen gültigen AFS-Token verfügen, den sie vom AFS-Authentifizierungsservice der lokalen Zelle erhielten.

Die dritte Systemverwaltungsgruppe, **system:administrators**, enthält eine kleine Gruppe von Administratoren, die über umfangreiche Berechtigungen in der Zelle verfügen. Sie müssen diese Gruppe nicht generell in Ihre ACLs stellen, da die Mitglieder der Gruppe in jeder ACL immer über die **a** (**administer**)-Berechtigung verfügen, selbst wenn die Gruppe nicht darin aufgeführt wird.

Aktivieren des Zugriffs auf Unterverzeichnisse

Ein Benutzer muß über die **l**-Berechtigung für ein Verzeichnis verfügen, um in irgendeiner Weise auf die jeweiligen Unterverzeichnisse zugreifen zu können. Selbst wenn Benutzer über umfangreiche Berechtigungen für ein Unterverzeichnis verfügen, können Sie darauf nicht zugreifen, wenn die ACL des Elternverzeichnisses die **l**-Berechtigung nicht erteilt.

Sie können die **l**-Berechtigung auf eine der drei folgenden Arten erteilen: Erteilung für eine Systemgruppe (**system:anyuser** oder **system:authuser**), Erteilung für einen einzelnen Benutzer oder Erteilung für eine oder mehrere Gruppen von Benutzern, die von Ihnen oder von anderen Benutzern definiert wurden (siehe „Kapitel 5. Verwendung von Gruppen” auf Seite 53). Die Erteilung der **l**-Berechtigung für die Gruppe **system:anyuser** ist dabei die einfachste Möglichkeit, und diese ist im allgemeinen sicher, da die Berechtigung nur Benutzern ermöglicht, den Inhalt des Verzeichnisses aufzulisten, nicht aber die Dateien darin zu lesen. Wenn Sie nur lokal authentifizierten Benutzern ermöglichen möchten, den Inhalt eines Verzeichnisses aufzulisten, ersetzen Sie die Gruppe **system:anyuser** durch die Gruppe **system:authuser**. Der Systemadministrator hat möglicherweise bereits einen Eintrag in der ACL Ihres Ausgangsverzeichnisses erstellt, der der Gruppe **system:anyuser** die Berechtigungen **r** und **l** erteilt.

Erweitern des Zugriffs auf Serviceprozesse

Es ist manchmal erforderlich, der Gruppe **system:anyuser** umfangreichere Berechtigungen zu erteilen, so daß Prozesse, die Druck- und Postzustellungsservices zur Verfügung stellen, korrekt ausgeführt werden können. Zum Beispiel ist für Druckprozesse zusätzlich zur **l**-Berechtigung manchmal die **r**-Berechtigung erforderlich. Für einen Postzustellungsprozeß ist möglicherweise die **i**-Berechtigung erforderlich, um neue Nachrichten in das Postverzeichnis zu stellen. Der Systemadministrator hat wahrscheinlich bereits die erforderlichen ACL-Einträge erstellt. Wenn Sie einen ACL-Eintrag bemerken, dessen Zweck unklar ist, fragen Sie den Systemadministrator dazu, bevor Sie den Eintrag entfernen.

Erweitern des Zugriffs auf Benutzer fremder Zellen

Die einzige Möglichkeit, Benutzern fremder Zellen, die über keinen Benutzereintrag in Ihrer Zelle verfügen, einen Zugriff zu erteilen, ist, die Gruppe **system:anyuser** in eine ACL zu stellen. Beachten Sie jedoch, daß durch diesen Eintrag der Zugriff so erweitert wird, daß er für jeden Benutzer gilt, der auf Ihre Zelle zugreifen kann, und nicht nur für die AFS-Benutzer fremder Zellen, für die dieser Schritt durchgeführt werden soll.

Anzeigen einer ACL

Zum Anzeigen der ACL, die einer Datei oder einem Verzeichnis zugeordnet ist, führen Sie den Befehl **fs listacl** aus.

Hinweis für Benutzer des AFS/DFS Migration Toolkit: Wenn die Maschine, auf der Sie den Befehl **fs listacl** ausführen, so konfiguriert ist, daß der Zugriff auf einen DFS-Dateibereich einer DCE-Zelle über das AFS/DFS Migration Toolkit erfolgt, können Sie mit dem Befehl die ACL in DFS-Dateien und -Verzeichnissen anzeigen. Wenn die ACL eines initialen Containers (Initial Container) oder eines initialen Objekts (Initial Object) eines DFS-Verzeichnisses anstelle der regulären ACL angezeigt werden soll, fügen Sie dem Befehl **fs listacl** die Markierung **-id** oder **-if** hinzu. Wenn Sie weitere Informationen hierzu benötigen, wenden Sie sich an den Systemadministrator. Der Befehls-Interpreter für **fs**-Befehle ignoriert die Markierungen **-id** und **-if**, wenn Sie diese beim Anzeigen einer AFS-ACL hinzufügen.

Vorgehensweise beim Anzeigen einer ACL

1. Führen Sie den Befehl **fs listacl** aus.

   ```
   % fs listacl [<Verzeichnis-/Dateipfad>+]
   ```

   Dabei gilt folgendes:

   la Ist ein akzeptabler Alias für **listacl** (und **lista** ist die kürzeste akzeptable Abkürzung).

   Verzeichnis-/Dateipfad
   Benennt eine oder mehrere Dateien oder Verzeichnisse, für die die ACL angezeigt werden soll. Für eine Datei wird die ACL im entsprechenden Verzeichnis angezeigt. Wenn Sie dieses Argument weglassen, gilt die Ausgabe für das aktuelle Arbeitsverzeichnis. Partielle Pfadnamen beziehen sich auf das aktuelle Arbeitsverzeichnis. Sie können auch die folgende Schreibweise - alleine oder als Teil eines Pfadnamens - verwenden:

   . (Ein einzelner Punkt). Gibt das aktuelle Arbeitsverzeichnis an.

   .. (Zwei Punkte). Geben das Elternverzeichnis des aktuellen Arbeitsverzeichnisses an.

***** (Stern). Steht für jede Datei und jedes Unterverzeichnis im aktuellen Arbeitsverzeichnis. Die für eine Datei angezeigte ACL ist immer dieselbe wie für das entsprechende Verzeichnis, die ACL für jedes Unterverzeichnis kann jedoch davon abweichen.

Die Ausgabe für jede Datei oder jedes Verzeichnis, die oder das für *Verzeichnis-/Dateipfad* angegeben wurde, beginnt mit der folgenden Überschrift:

```
Access list for  dir/file path is
```

Die Überschrift `Normal rights` wird in der nächsten Zeile angezeigt. Darauf folgen Zeilen, die jeweils ein Wertepaar bestehend aus Benutzer- oder Gruppenname und einer Menge an Berechtigungen sind. Die Berechtigungen werden als einfache Buchstaben angegeben (siehe „AFS-ACL-Berechtigungen" auf Seite 34) und immer in der Reihenfolge **rlidwka**. Wenn es negative Berechtigungen gibt, wird als nächstes die Überschrift `Negative rights` angezeigt, unter der Paare negativer Berechtigungen aufgeführt werden.

Wenn die folgende Fehlernachricht anstelle einer ACL emittiert wird, verfügen Sie nicht über die erforderlichen Berechtigungen, um eine ACL anzuzeigen. Um einen Verzeichnisnamen als Argument *Verzeichnis-/Dateipfad* angeben zu können, muß die **l** (**lookup**)-Berechtigung in der ACL vorliegen. Um einen Dateinamen angeben zu können, müssen Sie auch über die **r** (**read**)-Berechtigung in der ACL des entsprechenden Verzeichnisses verfügen.

```
fs: You don't have the required access permissions on 'dir/file path'
```

Beispiel: Anzeigen der ACL in einem Verzeichnis

Im folgenden Beispiel wird die ACL für das Ausgangsverzeichnis des Benutzers **terry** in der Zelle für die Firma ABC Corporation angezeigt:

```
% fs la /afs/abc.com/usr/terry
Access list for /afs/abc.com/usr/terry is
Normal rights:
   system:authuser rl
   pat rlw
   terry rlidwka
Negative rights:
   terry:other-dept rl
   jones rl
```

Dabei sind **pat**, **terry** und **jones** einzelne Benutzer, **system:authuser** eine Systemverwaltungsgruppe und **terry:other-dept** eine Gruppe, dessen Eigner **terry** ist. Die Liste der normalen Berechtigungen erteilt **terry** alle Berechtigungen, **pat** die Berechtigungen **rlw** und den Mitgliedern der Gruppe **system:authuser** die Berechtigungen **rl**.

Die Liste der negativen Berechtigungen verweigert **jones** und den Mitgliedern der Gruppe **terry:other-dept** die Berechtigungen **rl**. Durch diese Einträge wird effektiv verhindert, daß diese Benutzer in irgendeiner Weise auf das Aus-

gangsverzeichnis von **terry** zugreifen können. Sie setzen die Berechtigungen **rl** außer Kraft, die auf die Gruppe **system:authuser** erweitert wurden. Dies ist der einzige Eintrag in der Liste der normalen Berechtigungen in der ACL, der sich auf sie auswirken kann.

Beispiel: Anzeigen der ACLs in mehreren Verzeichnissen

Das folgende Beispiel veranschaulicht, wie Sie Pfadnamen auf verschiedene Arten und Weisen angeben können und wie die Ausgabe für mehrere Verzeichnisse dargestellt wird. In dem Beispiel werden die ACLs für drei Verzeichnisse angezeigt: das aktuelle Arbeitsverzeichnis (ein Unterverzeichnis des Ausgangsverzeichnisses des Benutzers **terry**), das Ausgangsverzeichnis für Benutzer **pat** und ein weiteres Unterverzeichnis des Ausgangsverzeichnisses von **terry** mit dem Namen **plans**.

```
% fs listacl  .  /afs/abc.com/usr/pat  ../plans
Access list for . is
Normal rights:
   system:anyuser rl
   pat:dept rliw
Access list for /afs/abc.com/usr/pat is
Normal rights:
   system:anyuser rl
   pat rlidwka
   terry rliw
Access list for ../plans is
Normal rights:
   terry rlidwka
   pat rlidw
```

Ändern einer ACL

Zum Hinzufügen, Entfernen oder Editieren von ACL-Einträgen verwenden Sie den Befehl **fs setacl**. Standardmäßig werden mit diesem Befehl Einträge im Abschnitt mit den normalen Berechtigungen in der ACL bearbeitet. Um Einträge im Abschnitt mit den negativen Berechtigungen zu bearbeiten, fügen Sie die Markierung **-negative** hinzu. Anweisungen dazu finden Sie unter „Hinzufügen, Entfernen oder Editieren negativer ACL-Berechtigungen” auf Seite 45.

Sie können jede ACL ändern, in der Sie bereits über die **a**-Berechtigung verfügen. Sie verfügen für jedes Verzeichnis, dessen Eigner sind, immer über die **a**-Berechtigung in der ACL. Dies gilt selbst dann, wenn Sie diese Berechtigung versehentlich aus der ACL entfernen. (Mit dem Befehl **ls -ld** können Sie den Verzeichniseigner anzeigen.) Der Systemadministrator legt Sie normalerweise als Eigner Ihres Ausgangsverzeichnisses und dessen Unterverzeichnisse fest, und möglicherweise sind Sie Eigner weiterer Verzeichnisse.

Wenn bereits ein ACL-Eintrag für den angegebenen Benutzer oder die Gruppe vorhanden ist, werden die vorhandenen Berechtigungen vollständig durch neue Berechtigungen ersetzt. Die neuen Berechtigungen werden nicht hinzu-

gefügt. Anders ausgedrückt: Wenn Sie den Befehl **fs setacl** ausführen, müssen Sie alle Berechtigungen angeben, die einem Benutzer oder einer Gruppe erteilt werden sollen.

Hinweis für Benutzer des AFS/DFS Migration Toolkit: Wenn die Maschine, auf der Sie den Befehl **fs setacl** ausführen, so konfiguriert ist, daß der Zugriff auf einen DFS-Dateibereich einer DCE-Zelle über das AFS/DFS Migration Toolkit erfolgt, können Sie mit dem Befehl die ACL in DFS-Dateien und -Verzeichnissen definieren. Wenn die ACL eines initialen Containers (Initial Container) oder eines initialen Objekts (Initial Object) eines DFS-Verzeichnisses anstelle der regulären ACL definiert werden soll, fügen Sie dem Befehl **fs setacl** die Markierung **-id** oder **-if** hinzu. Wenn Sie weitere Informationen hierzu benötigen, wenden Sie sich an den Systemadministrator. Der Befehls-Interpreter für **fs**-Befehle ignoriert die Markierungen **-id** und **-if**, wenn Sie diese beim Definieren einer AFS-ACL hinzufügen.

Hinzufügen, Entfernen oder Editieren normaler ACL-Berechtigungen

Führen Sie den Befehl **fs setacl** aus, um Einträge im Abschnitt mit den normalen Berechtigungen in der ACL zu editieren. Geben Sie zum Entfernen eines Eintrags die Kurzform **none** als Berechtigungen an. Wenn bereits ein ACL-Eintrag für einen Benutzer oder eine Gruppe vorhanden ist, werden die Berechtigungen in einem vorhandenen Eintrag vollständig durch die Berechtigungen ersetzt, die Sie angeben.

```
% fs setacl -dir <Verzeichnis>+ -acl <Zugriffslisteneinträge>+
```

Dabei gilt folgendes:

sa Ist ein akzeptabler Alias für **setacl** (und **seta** ist die kürzeste akzeptable Abkürzung).

-dir Benennt ein oder mehrere Verzeichnisse, für das bzw. die die ACL-Einträge gelten sollen, die durch das Argument **-acl** definiert sind. Partielle Pfadnamen beziehen sich auf das aktuelle Arbeitsverzeichnis. Sie können auch die folgende Schreibweise - alleine oder als Teil eines Pfadnamens - verwenden:

- **.** (Ein einzelner Punkt). Wenn nur der Punkt verwendet wird, wird die ACL für das aktuelle Arbeitsverzeichnis definiert.
- **..** (Zwei Punkte). Wenn nur die Punkte verwendet werden, wird die ACL für das Elternverzeichnis des aktuellen Arbeitsverzeichnisses definiert.
- ***** (Stern). Definiert die ACL in jedem der Unterverzeichnisse im aktuellen Arbeitsverzeichnis. Vor dem Stern muß der Schalter **-dir** stehen, da er potentiell mehrere Verzeichnisse bezeichnet. Der Befehls-Interpreter für **fs**-Befehle generiert die folgende Fehlernachricht für jede Datei im Verzeichnis:

```
fs: 'filename': Not a directory
```

Wenn Sie nur einen Verzeichnis- oder Dateinamen angeben, können Sie die Schalter **-dir** und **-acl** weglassen. Weitere Informationen dazu, in welchen Fällen bestimmte Schalter weggelassen werden können, enthält „Anhang B. AFS-Befehlssyntax und Online-Hilfefunktion” auf Seite 81.

-acl Gibt einen oder mehrere ACL-Einträge an. Dabei ist jeder Eintrag ein Wertepaar bestehend aus einem Benutzer- oder Gruppennamen und einer Menge von Berechtigungen. Die einzelnen Wertepaare und die zwei Teile jedes Paars müssen mit mindestens einem Leerzeichen voneinander getrennt werden.

Zum Definieren der Berechtigungen geben Sie folgendes an:

- Entweder: Einen oder mehrere Buchstaben, die für die Standardberechtigungen oder die zusätzlichen Berechtigungen stehen (**rlidwka** und **ABCDEFGH**), in beliebiger Reihenfolge.
- Oder: Eine der vier Kurzformen:
  - **all** (gleichbedeutend mit **rlidwka**)
  - **none** (entfernt den Eintrag)
  - **read** (gleichbedeutend mit **rl**)
  - **write** (gleichbedeutend mit **rlidwk**)

Sie können Benutzer- und Gruppeneinträge in einer einzelnen Befehlszeile kombinieren. Sie können auch die beiden Schreibweisen - einzelne Buchstaben und die Kurzformen - kombinieren, aber nicht innerhalb eines einzelnen Paars.

Beispiel: Hinzufügen eines einzelnen ACL-Eintrags

Mit jedem der folgenden Beispielbefehle werden Benutzer **pat** die Berechtigungen **r** und **l** in der ACL des Unterverzeichnisses **notes** des aktuellen Arbeitsverzeichnisses erteilt. Sie veranschaulichen, wie die Schalter **-dir** und **-acl** weggelassen werden können, wenn nur ein Verzeichnis benannt wird.

```
% fs sa notes pat rl
% fs sa pat read
```

Beispiel: Definition mehrerer ACL-Einträge in einem Verzeichnis

In folgendem Beispiel wird die ACL für das aktuelle Arbeitsverzeichnis editiert. Der Eintrag für die Gruppe **system:anyuser** wird entfernt, und zwei Einträge werden hinzugefügt: Mit einem Eintrag werden den Mitgliedern der Gruppe **terry:colleagues** alle Berechtigungen außer **a** erteilt. Mit dem anderen Eintrag werden der Gruppe **system:authuser** die Berechtigungen **r** und **l** erteilt.

```
% fs sa -dir . -acl  system:anyuser none  terry:colleagues write  \
        system:authuser rl
```

Hinzufügen, Entfernen oder Editieren negativer ACL-Berechtigungen

Führen Sie den Befehl **fs setacl** mit der Markierung **-negative** aus, um Einträge im Abschnitt mit den negativen Berechtigungen in der ACL zu editieren. Geben Sie zum Entfernen eines Eintrags die Kurzform **none** als Berechtigungen an. Wenn bereits ein ACL-Eintrag für einen Benutzer oder eine Gruppe vorhanden ist, werden die Berechtigungen in einem vorhandenen Eintrag vollständig durch die Berechtigungen ersetzt, die Sie angeben.

```
% fs setacl -dir <Verzeichnis>+ -acl <Zugriffslisteneinträge >+  -negative
```

Dabei gilt folgendes:

sa Ist ein akzeptabler Alias für **setacl** (und **seta** ist die kürzeste akzeptable Abkürzung).

-dir Benennt ein oder mehrere Verzeichnisse, für das bzw. die die ACL-Einträge für negative Berechtigung gelten sollen, die durch das Argument **-acl** definiert sind. Eine detaillierte Beschreibung akzeptabler Werte enthält der Abschnitt „Hinzufügen, Entfernen oder Editieren normaler ACL-Berechtigungen” auf Seite 43.

-acl Gibt einen oder mehrere ACL-Einträge an. Dabei ist jeder Eintrag ein Wertepaar bestehend aus einem Benutzer- oder Gruppennamen und einer Menge von Berechtigungen. Die einzelnen Wertepaare und die zwei Teile jedes Paars müssen mit mindestens einem Leerzeichen voneinander getrennt werden. Eine detaillierte Beschreibung akzeptabler Werte enthält der Abschnitt „Hinzufügen, Entfernen oder Editieren normaler ACL-Berechtigungen” auf Seite 43. Achten Sie darauf, daß die übliche Bedeutung jeder Berechtigung umgekehrt wird.

-negative
Stellt die Einträge, die durch das Argument **-acl** definiert sind, in den Abschnitt mit den negativen Berechtigungen in der ACL für jedes Verzeichnis, das durch das Argument **-dir** angegeben wurde.

Beispiel: Definieren eines Eintrags im Abschnitt mit den negativen Berechtigungen

Benutzerin **terry** erteilte der Gruppe **terry:team** sämtliche Zugriffsberechtigungen außer **a** für ihr Unterverzeichnis **plans**.

```
% cd /afs/abc.com/usr/terry
% fs listacl plans
Access control list for plans is
Normal rights:
    system:anyuser rl
    terry:team rlidwk
    terry  rlidwka
```

terry stellt jedoch fest, daß eines der Mitglieder der Gruppe, Benutzer **pat**, unkorrekte Änderungen an den Dateien vornahm. Um dies zu verhindern, ohne Benutzer **pat** aus der Gruppe zu entfernen oder die Berechtigungen für

die Gruppe **terry:team** zu ändern, erstellt **terry** einen Eintrag im Abschnitt mit den negativen Berechtigungen in der ACL, mit dem Benutzer **pat** die Berechtigungen **w** und **d** verweigert werden:

```
% fs setacl plans pat wd -negative
% fs listacl plans
Access control list for plans is
Normal rights:
    system:anyuser rl
    terry:team rlidwk
    terry: rlidwka
Negative rights:
    pat wd
```

Beispiel: Wiederherstellen des Zugriffs durch Entfernen eines Eintrags aus dem Abschnitt mit den negativen Berechtigungen

Im vorherigen Beispiel stellte Benutzer **terry** Benutzer **pat** für das Unterverzeichnis **plans** in den Abschnitt mit den negativen Berechtigungen in der ACL. Das Ergebnis war jedoch nicht zufriedenstellend. Benutzer **pat** versicherte jetzt, keine Dateien mehr zu ändern. Um dem Benutzer **pat** zu ermöglichen, alle Berechtigungen zu nutzen, die den Mitgliedern der Gruppe **terry:team** erteilt wurden, entfernt **terry** den Eintrag **pat** wieder aus dem Abschnitt mit den negativen Berechtigungen in der ACL.

```
% fs setacl plans pat none -negative
% fs listacl plans
Access control list for plans is
Normal rights:
    system:anyuser rl
    terry:team rlidwk
    terry rlidwka
```

Vollständiges Ersetzen einer ACL

Manchmal ist es am einfachsten, den Inhalt einer ACL komplett zu löschen, bevor neue Berechtigungen in ihr definiert werden. Dies ist zum Beispiel der Fall, wenn es durch die Mischung aus normalen und negativen Berechtigungen schwer ersichtlich ist, wie ihre Interaktion sich auf den Zugriff auf das Verzeichnis auswirkt. Um eine ACL vollständig zu löschen, während Sie neue Einträge definieren, fügen Sie dem Befehl **fs setacl** die Markierung **-clear** hinzu. Wenn Sie diese Markierung hinzufügen, können Sie Einträge entweder im Abschnitt mit den normalen oder im Abschnitt mit den negativen Berechtigungen in der ACL erstellen, aber nicht in beiden Abschnitten gleichzeitig.

Denken Sie daran, daß Sie einen Eintrag für sich selbst erstellen. Als Eigner des Verzeichnisses verfügen Sie stets über die **a** (**administer**)-Berechtigung, die erforderlich ist, um einen gelöschten Eintrag zu ersetzen. Die Auswirkungen durch einen fehlenden ACL-Eintrag können sehr verwirrend sein, und lassen oft nicht direkt darauf schließen, daß die Ursache des Problems ein fehlender Eintrag ist. Insbesondere können Sie, wenn die **l** (**lookup**)-Berechtigung fehlt,

die Kurzform in Pfadnamen nicht verwenden (wie zum Beispiel einen Punkt für das aktuelle Arbeitsverzeichnis oder zwei Punkte für das Elternverzeichnis).

Vollständiges Ersetzen einer ACL

Führen Sie den Befehl **fs setacl** mit der Markierung **-clear** aus, um die ACL vollständig zu löschen, bevor entweder normale oder negative Berechtigungen erteilt werden. Da Sie dem Eigner des Verzeichnisses alle Berechtigungen erteilen müssen, ist es in den meisten Fällen besser, an diesem Punkt normale Berechtigungen zu definieren.

```
% fs setacl -dir <Verzeichnis>+ -acl <Zugriffslisteneinträge >+ -clear  [-negative]
```

Dabei gilt folgendes:

sa Ist ein akzeptabler Alias für **setacl** (und **seta** ist die kürzeste akzeptable Abkürzung).

-dir Benennt ein oder mehrere Verzeichnisse, für das bzw. die die ACL-Einträge gelten sollen, die durch das Argument **-acl** definiert sind. Eine detaillierte Beschreibung akzeptabler Werte enthält der Abschnitt „Hinzufügen, Entfernen oder Editieren normaler ACL-Berechtigungen” auf Seite 43.

-acl Gibt einen oder mehrere ACL-Einträge an. Dabei ist jeder Eintrag ein Wertepaar bestehend aus einem Benutzer- oder Gruppennamen und einer Menge von Berechtigungen. Die einzelnen Wertepaare und die zwei Teile jedes Paars müssen mit mindestens einem Leerzeichen voneinander getrennt werden. Achten Sie darauf, daß dem Eigner des Verzeichnisses alle Berechtigungen erteilt werden müssen. Eine detaillierte Beschreibung akzeptabler Werte enthält der Abschnitt „Hinzufügen, Entfernen oder Editieren normaler ACL-Berechtigungen” auf Seite 43.

-clear Entfernt alle Einträge aus jeder ACL, bevor die Einträge erstellt werden, die durch das Argument **-acl** angegeben werden.

-negative
Stellt die Einträge, die durch das Argument **-acl** definiert sind, in den Abschnitt mit den negativen Berechtigungen in jeder ACL.

Beispiel: Ersetzen einer ACL

Im folgenden Beispiel wird der Inhalt der ACL für das aktuelle Arbeitsverzeichnis vollständig gelöscht, und es werden Einträge erstellt, mit denen Benutzer **terry** alle Berechtigungen und Benutzer **pat** alle Berechtigungen außer **a** erteilt werden.

```
% fs setacl . terry all pat write -clear
% fs listacl .
Access control list for . is
Normal rights:
  terry rlidwka
  pat rlidwk
```

Kopieren von ACLs von einem Verzeichnis in ein anderes

Mit dem Befehl **fs copyacl** wird die ACL eines Quellenverzeichnisses in ein oder mehrere Zielverzeichnisse kopiert. Dies hat keinerlei Auswirkungen auf die ACL des Quellenverzeichnisses. Es werden jedoch bei den ACLs der Zielverzeichnisse folgende Änderungen vorgenommen:

- Wenn ein Eintrag in der ACL des Quellenverzeichnisses nicht in der ACL des Zielverzeichnisses vorhanden ist, kopiert der Befehl diesen Eintrag in die Ziel-ACL.
- Wenn ein Eintrag in der ACL des Zielverzeichnisses nicht auch in der ACL des Quellenverzeichnisses vorhanden ist, entfernt der Befehl den Eintrag nicht, es sei denn, die Markierung **-clear** wird hinzugefügt, die die ACL im Zielverzeichnis komplett überschreibt.
- Wenn ein Eintrag in beiden ACLs vorhanden ist, ändert der Befehl den Eintrag in der ACL des Zielverzeichnisses dahingehend, daß er mit dem Eintrag in der ACL des Quellenverzeichnisses übereinstimmt.

Um eine ACL zu kopieren, müssen Sie über die **l**-Berechtigung in der ACL des Quellenverzeichnisses und über die **a**-Berechtigung in der ACL jedes Zielverzeichnisses verfügen. Wenn Sie das Quellenverzeichnis durch Benennen einer darin enthaltenen Datei identifizieren, müssen Sie darüber hinaus über die **r**-Berechtigung in der ACL des Quellenverzeichnisses verfügen. Zum Anzeigen der Berechtigungen, über die Sie in den beiden Verzeichnissen verfügen, verwenden Sie den Befehl **fs listacl** (siehe die Beschreibung unter „Anzeigen einer ACL” auf Seite 40).

Hinweis für Benutzer des AFS/DFS Migration Toolkit: Wenn die Maschine, auf der Sie den Befehl **fs copyacl** ausführen, so konfiguriert ist, daß der Zugriff auf einen DFS-Dateibereich einer DCE-Zelle über das AFS/DFS Migration Toolkit erfolgt, können Sie mit dem Befehl auch ACLs zwischen DFS-Dateien und -Verzeichnissen hin und her kopieren. Der Befehl enthält die Markierungen **-id** und **-if** zur Änderung der ACLs des initialen Containers (Initial Container) und des initialen Objekts (Initial Object) eines DFS-Verzeichnisses sowie die normale ACL. Wenn Sie weitere Informationen benötigen, wenden Sie sich an den Systemadministrator. Sie können ACLs nicht zwischen AFS- und DFS-Verzeichnissen hin und her kopieren, da sie unterschiedliche ACL-Formate verwenden. Der Befehls-Interpreter für **fs**-Befehle ignoriert die Markierungen **-id** und **-if**, wenn Sie diese beim Kopieren von AFS-ACLs hinzufügen.

Kopieren einer ACL von einem Verzeichnis in ein anderes

Führen Sie den Befehl **fs copyacl** aus, um die ACL eines Quellenverzeichnisses in die ACL eines oder mehrerer Zielverzeichnisse zu kopieren.

```
% fs copyacl -fromdir <Quellenverzeichnis> -todir <Zielverzeichnis>+  \
            [-clear]
```

Dabei gilt folgendes:

co Ist die kürzeste akzeptable Abkürzung für **copyacl**.

-fromdir
Benennt das Quellenverzeichnis, aus dem die ACL kopiert werden soll. Partielle Pfadnamen beziehen sich auf das aktuelle Arbeitsverzeichnis. Wenn dieses Argument eine Datei benennt, wird die ACL aus dem entsprechenden Verzeichnis kopiert.

-todir Benennt jedes Zielverzeichnis, an das die ACL des Quellenverzeichnisses kopiert werden soll. Partielle Pfadnamen beziehen sich auf das aktuelle Arbeitsverzeichnis. Dateinamen werden nicht akzeptiert.

-clear Überschreibt die ACL jedes Zielverzeichnisses vollständig mit der Quellen-ACL.

Beispiel: Kopieren einer ACL von einem Verzeichnis in ein anderes

In diesem Beispiel kopiert die Benutzerin **terry** die ACL aus ihrem Ausgangsverzeichnis (dem aktuellen Arbeitsverzeichnis) in dessen Unterverzeichnis **plans**. Sie beginnt damit, beide ACLs anzuzeigen.

```
% fs listacl . plans
 Access list for . is
 Normal rights:
   terry rlidwka
   pat rlidwk
   jones rl
 Access list for plans is
 Normal rights:
   terry rlidwka
   pat rl
   smith rl

% fs copyacl -from . -to plans

% fs listacl . plans
 Access list for . is
 Normal rights:
   terry rlidwka
   pat rlidwk
   jones rl
 Access list for plans is
 Normal rights:
```

```
terry rlidwka
pat rlidwk
jones rl
smith rl
```

Verwendung der UNIX-Modusbits durch AFS

Obwohl AFS-Daten hauptsächlich durch ACLs schützt, und nicht durch Modusbits, werden die Modusbits nicht gänzlich ignoriert. Eine Erläuterung dazu, wie das Verwenden von Modusbits im UNIX-Dateisystem funktioniert, würde den Rahmen dieser Veröffentlichung sprengen. Die folgende Diskussion setzt daher voraus, daß Sie die Funktionsweise von Modusbits verstehen. Wenn Sie darüberhinaus Erläuterungen benötigen, lesen Sie die entsprechenden Informationen in der UNIX-Dokumentation. Gleichermaßen werden in der folgenden Diskussion nicht die Funktionsweisen von setuid, setgid oder sticky Bits erläutert. Wenn Sie Erläuterungen zu den Funktionsweisen dieser Bits in bezug auf AFS-Dateien benötigen, lesen Sie die entsprechenden Informationen in der Veröffentlichung *AFS Administration Guide*, oder wenden Sie sich an den Systemadministrator.

AFS verwendet die UNIX-Modusbits in der folgenden Art und Weise:

- Das initiale Bit wird zur Unterscheidung von Dateien und Verzeichnissen verwendet. Dies ist das Bit, das als erstes in der Ausgabe des Befehls **ls -l** angezeigt wird und den Silbentrennungsstrich (**-**) für eine Datei oder den Buchstaben `d` für ein Verzeichnis anzeigt.
- AFS verwendet keines der Modusbits für ein Verzeichnis. Der Verzeichniszugriff wird ausschließlich über die AFS-ACL gesteuert.
- Für eine Datei interagiert die Eigner-Bitmenge (die erste Bitmenge) mit den ACL-Einträgen, die sich auf folgende Art und Weise auf die Datei beziehen. AFS verwendet die Gruppen- oder Weltmodusbits (zweite und dritte Menge) der Modusbits überhaupt nicht.
  - Wenn das erste **r**-Modusbit nicht gesetzt ist, kann keiner (einschließlich Eigner) die Datei lesen, unabhängig davon, welche Berechtigungen in der ACL definiert sind. Wenn das Bit gesetzt ist, benötigen Benutzer auch die Berechtigungen **r** und **l** in der ACL des Dateienverzeichnisses, um die Datei zu lesen.
  - Wenn das erste **w**-Modusbit nicht gesetzt ist, kann keiner (einschließlich Eigner) die Datei ändern. Wenn das Bit **w** gesetzt ist, benötigen Benutzer auch die Berechtigungen **w** und **l** in der ACL des Verzeichnisses der Datei, um die Datei zu ändern.
  - Es gibt keine ACL-Berechtigung, die dem Modusbit **x** direkt entspricht. Um jedoch eine in AFS gespeicherte Datei auszuführen, muß der Benutzer auch über die Berechtigungen **r** und **l** in der ACL des Verzeichnisses der Datei verfügen.

Wenn Sie den UNIX-Befehl **chmod** für eine AFS-Datei oder ein AFS-Verzeichnis ausführen, ändert AFS die Bits entsprechend. Um die Modusbits einer Datei ändern zu können, müssen Sie über die AFS-Berechtigung **w** in der ACL des Verzeichnisses der Datei verfügen. Um die Modusbits eines Verzeichnisses zu ändern, müssen Sie über die Berechtigungen **d**, **i** und **l** in der ACL verfügen.

Beispiel: Inaktivieren des Schreibzugriffs für eine Datei

Angenommen, **terry** ist Vorsitzende eines Komitees, das ein Schriftstück verfaßt. Nachdem den einzelnen Abschnitten des Schriftstücks zugestimmt wurde, schaltet sie den Schreibzugriff für diese Datei aus, damit keine weiteren Änderungen daran vorgenommen werden können. Zum Beispiel schaltet der folgende Befehl des Typs **chmod** die **w**-Modusbits in der Datei **proposal.chap2** aus. Dadurch werden Änderungen der Datei verhindert, unabhängig davon, welche Berechtigungen in der ACL des Verzeichnisses erteilt werden.

```
% chmod -w proposal.chap2
% ls -l
-rw-r--r--  1 terry     573 Nov 10 09:57 conclusion
-r--r--r--  1 terry     573 Nov 15 10:34 intro
-r--r--r--  1 terry     573 Dec  1 15:07 proposal.chap2
-rw-r--r--  1 terry     573 Nov 10 09:57 proposal.chap3
-rw-r--r--  1 terry     573 Nov 10 09:57 proposal.chap4
```

Kapitel 5. Verwendung von Gruppen

In diesem Kapitel wird erklärt, wie Gruppen zu verwenden sind, und es werden verschiedene Arten ihrer Verwendung beschrieben.

Informationen zu Gruppen

Eine AFS-*Gruppe* ist eine Liste spezieller Benutzer, die Sie in Zugriffssteuerungslisten (ACLs) unterbringen können. Mit Gruppen lassen sich ACLs leichter verwalten. Statt für jeden Benutzer eine ACL individuell zu erstellen, können Sie für eine Gruppe, zu der die Benutzer gehören, einen einzigen Eintrag erstellen. In ähnlicher Weise können Sie einen Benutzerzugriff auf viele Verzeichnisse einmalig gestatten, indem Sie den Benutzer zu einer Gruppe hinzufügen, die in den jeweiligen ACLs erscheint.

AFS-Client-Maschinen können ebenfalls zu einer Gruppe gehören. Jeder, der sich bei der Maschine angemeldet hat, übernimmt die Berechtigungen, die der Gruppe in einer ACL erteilt wurden, auch wenn er bei AFS nicht authentifiziert ist.Im allgemeinen sind Maschinengruppen nur für Systemadministratoren für spezielle Zwecke nützlich, wie das Erfüllen von Lizenzvereinbarungen, die Ihre Zelle mit Softwarelieferanten hat. Sprechen Sie mit Ihrem Systemadministrator, bevor Sie eine Client-Maschine zu einer Gruppe hinzufügen oder mit Hilfe einer Maschinengruppe in einer ACL einsetzen.

Informationen zum AFS-Dateizugriffsschutz und über das Hinzufügen von Gruppen zu ACLs finden Sie in „Kapitel 4. Zugriffsschutz für Verzeichnisse und Dateien” auf Seite 33.

Vorschläge zum effektiven Einsatz von Gruppen

Es gibt drei typische Methoden, um Gruppen zu verwenden, jede für einen bestimmten Zweck: private Verwendung, gemeinsame Verwendung und Gruppenverwendung. Nachstehend werden nur Vorschläge dargestellt. Es steht Ihnen natürlich frei, auf welche Weise Sie Gruppen einsetzen.

- *Private Verwendung*: Sie erstellen eine Gruppe und bringen Sie in der ACL Ihres eigenen Verzeichnisses unter, ohne die Mitglieder der Gruppe zu informieren, daß diese zu ihr gehören. Die Mitglieder bemerken nur, daß sie auf das Verzeichnis auf bestimmte Art zugreifen können oder nicht. Sie behalten über die Gruppe solange die alleinige administrative Kontrolle, wie Sie der Eigner sind.

  Die Existenz der Gruppe und die Identität ihrer Mitglieder sind nicht geheim. Andere Benutzer können Namen der Gruppe in einer ACL sehen, wenn Sie den Befehl **fs listacl** verwenden, und sie können den Befehl **pts**

© Copyright IBM Corp. 1989, 2000

membership verwenden, um sich die Gruppen anzeigen zu lassen, zu denen sie selbst gehören. Sie können jedoch, wie in „Schützen von Gruppeninformationen" auf Seite 65 beschrieben, festlegen, wer sich die Mitglieder der Gruppe anzeigen lassen kann.

- *Gemeinsame Verwendung*: Sie informieren die Mitglieder der Gruppe, daß sie zur Gruppe gehören, sind jedoch der alleinige Eigner und Administrator der Gruppe. Zum Beispiel kann der Manager einer Workgroup aus allen Mitglieder der Workgroup eine Gruppe bilden und sie auffordern, diese Gruppe in den ACLs von Verzeichnissen mit Informationen zu verwenden, die sie mit anderen Gruppenmitgliedern gemeinsam benutzen möchten.

  Anmerkung: Wenn Sie die Gruppe eines anderen in Ihren ACLs plazieren, kann der Eigner der Gruppe die Gruppenzugehörigkeit ändern, ohne Sie zu informieren. Irgendein anderer kann den Zugriff, ohne daß Sie es möchten, und ohne Ihr Wissen gestatten oder verbieten.

- *Gruppenverwendung*: Sie erstellen eine Gruppe und benutzen danach den Befehl **pts chown**, um das Eigentumsrecht an einer Gruppe — entweder einer anderen Gruppe oder der Gruppe selbst (der letzte Typ ist eine *Gruppe, die sich selbst gehört*) zuzuweisen. Sie informieren die Mitglieder der Eignergruppe, daß sie alle die untergeordnete Gruppe verwalten können. Anweisungen zum Befehl **pts chown** finden Sie in „So ändern Sie den Eigner einer Gruppe" auf Seite 63.

  Der Hauptvorteil des Kennzeichnens einer Gruppe als einen Eigner ist, daß sich mehrere Benutzer die Verantwortung für das Verwalten der Gruppe teilen. Eine einzelne Person muß nicht alle administrativen Aufgaben wahrnehmen, und wenn der ursprüngliche Eigner der Gruppe die Zelle verläßt, sind noch andere Personen da, die sie verwalten können.

  Jedoch kann jeder in der Eignergruppe Änderungen vornehmen, die andere negativ beeinflussen: das ungeeignete Hinzufügen oder Entfernen von Personen oder das Ändern in ein ausschließliches Eigentumsrecht dieser Personen der Gruppe. Diese Probleme können in einer sich selbst gehörenden Gruppe von sehr sensibler Art sein. Das Verwenden einer Eignergruppe funktioniert am besten, wenn alle Mitglieder einander kennen und vertrauen; es ist wahrscheinlich am klügsten, die Anzahl der Personen in einer Eignergruppe klein zu halten.

Gruppennamen

Die von Ihnen erstellten Gruppen müssen aus zwei Teilen bestehende Namen nach dem folgenden Format erhalten:

Eignername:*Gruppenname*

Der Präfix *Eignername* zeigt an, welchem Benutzer oder welcher Gruppe die Gruppe gehört (Namenskonventionen finden Sie in „So erstellen Sie eine

Gruppe" auf Seite 59). Der Teil *Gruppenname* zeigt den Zweck der Gruppe oder das allgemeine Interesse ihrer Mitglieder an. Gruppennamen müssen immer vollständig geschrieben werden, so daß ein kurzer *Gruppenname* am praktikabelsten ist. Namen wie **terry:1** und **terry:2**, die den Zweck der Gruppe nicht erkennen lassen, sind weniger nützlich als Namen wie **terry:project**.

Gruppen, die den Präfix *Eignername* nicht besitzen, treten möglicherweise in einigen ACLs auf; sie wurden ausschließlich durch Systemadministratoren erstellt. Alle von Ihnen erstellten Gruppen müssen einen Präfix *Eignername* besitzen.

Gruppenerstellungsquote

Standardmäßig können Sie 20 Gruppen erstellen, aber Ihr Systemadministrator kann, wenn es geeignet erscheint, Ihre *Gruppenerstellungsquote* ändern. Wenn Sie eine Gruppe erstellen, sinkt Ihre Gruppenquote um eins. Wenn eine von Ihnen erstellte Gruppe gelöscht wird, steigt Ihre Quote um eins, auch wenn Sie nicht mehr der Eigner sind. Sie können Ihre Quote nicht erhöhen, indem Sie das Eigentumsrecht an einer Gruppe jemand anderem übertragen, weil Sie immer als der Ersteller gespeichert sind.

Wenn Sie Ihre Gruppenerstellungsquote ausgeschöpft haben und trotzdem weitere Gruppen erstellen müssen, wenden Sie sich an Ihren Systemadministrator. Anweisungen für das Anzeigen Ihrer Gruppenerstellungsquote finden Sie in „So lassen Sie sich einen Gruppeneintrag anzeigen" auf Seite 57.

Anzeigen von Gruppeninformationen

Sie können die folgenden Befehle verwenden, um sich Informationen über Gruppen und die zu Ihnen gehörenden Benutzer anzeigen zu lassen:

- Um sich die Mitglieder einer Gruppe oder die Gruppen, zu denen ein Benutzer gehört, anzeigen zu lassen, verwenden Sie den Befehl **pts membership**.
- Um sich die Gruppen anzeigen zu lassen, die einem Benutzer oder einer Gruppe gehören, verwenden Sie den Befehl **pts listowned**.
- Um sich Basisinformationen über einen Benutzer oder eine Gruppe einschließlich des Namens, der AFS-ID, dem Ersteller und dem Eigner anzeigen zu lassen, verwenden Sie den Befehl **pts examine**.

Anmerkung: Die Systemverwaltungsgruppen **system:anyuser** und **system:authuser** erscheinen in keiner Gruppenzugehörigkeitsliste eines Benutzers, und der Befehl **pts membership** zeigt ihre Mitglieder nicht an. Weitere Informationen zu den Systemverwaltungsgruppen finden Sie in „Verwenden von Systemverwaltungsgruppen in ACLs" auf Seite 38.

So lassen Sie sich die Gruppenzugehörigkeit anzeigen

Verwenden Sie den Befehl **pts membership**, um sich die Mitglieder einer Gruppe oder die Gruppen, zu denen ein Benutzer gehört, anzeigen zu lassen.

```
% pts membership <Benutzer oder Gruppenname oder -ID>+
```

wobei *Benutzer oder Gruppenname oder -ID* den Namen oder die AFS-UID jedes Benutzers, für den die Gruppenzugehörigkeit angezeigt werden soll, oder den Namen oder die AFS-GID jeder Gruppe, deren Mitglieder angezeigt werden sollen, angibt. Beim Identifizieren einer Gruppe über ihre AFS-GID, stellen Sie der GID einen Silbentrennungsstrich (-) voran, um anzuzeigen, daß es sich um eine negative Nummer handelt.

Beispiel: Anzeigen der Mitglieder einer Gruppe

Das folgende Beispiel zeigt die Mitglieder der Gruppe **terry:team** an.

```
% pts membership terry:team
Members of terry:team (id: -286) are:
terry
smith
pat
johnson
```

Beispiel: Anzeigen der Gruppen, zu denen ein Benutzer gehört

Das folgende Beispiel zeigt die Gruppen an, zu denen die Benutzer **terry** und **pat** gehören.

```
% pts membership terry pat
Groups terry (id: 1022) is a member of:
smith:friends
pat:accounting
terry:team
Groups pat (id: 1845) is a member of:
pat:accounting
sam:managers
terry:team
```

So lassen Sie sich die Gruppen anzeigen, die einem Benutzer oder einer Gruppe gehören

Verwenden Sie den Befehl **pts listowned**, um sich die Gruppen anzeigen zu lassen, die einem Benutzer oder einer Gruppe gehören.

```
% pts listowned <Benutzer oder Gruppenname oder -ID>+
```

wobei *Benutzer oder Gruppenname oder -ID* den Namen oder die AFS-UID jedes Benutzers oder den Namen oder die AFS-GID jeder Gruppe, für die das Eigentumsrecht an der Gruppe angezeigt werden soll, angibt. Beim Identifizieren einer Gruppe über ihre AFS-GID, stellen Sie der GID einen Silbentrennungsstrich (-) voran, um anzuzeigen, daß es sich um eine negative Nummer handelt.

Beispiel: Anzeigen der Gruppen, die einer Gruppe gehören

Das folgende Beispiel zeigt die Gruppen an, die der Gruppe **terry:team** gehören.

```
% pts listowned -286
Groups owned by terry:team (id: -286) are:
terry:project
terry:planners
```

Beispiel: Anzeigen der Gruppen, die einem Benutzer gehören

Das folgende Beispiel zeigt die Gruppen an, die dem Benutzer **pat** gehören.

```
% pts listowned pat
Groups owned by pat (id: 1845) are:
pat:accounting
pat:plans
```

So lassen Sie sich einen Gruppeneintrag anzeigen

Verwenden Sie den Befehl **pts examine** um sich Basisinformationen über einen Benutzer oder eine Gruppe, einschließlich des Namens, der AFS-ID, dem Ersteller und dem Eigner anzeigen zu lassen.

```
% pts examine <Benutzer oder Gruppenname oder -ID>+
```

wobei *Benutzer oder Gruppenname oder -ID* den Namen oder die AFS-UID jedes Benutzers oder den Namen oder die AFS-GID jeder Gruppe, für die die Gruppeinformationen angezeigt werden soll, angibt. Beim Identifizieren einer Gruppe über ihre AFS-GID, stellen Sie der GID einen Silbentrennungsstrich (**-**) voran, um anzuzeigen, daß es sich um eine negative Nummer handelt.

Die Ausgabe enthält Informationen in den folgenden Feldern:

name Für Benutzer ist dies die beim Anmelden einzugebende Zeichenfolge. Für Maschinen ist der Name die IP-Adresse; eine Null im Adreßfeld dient als Platzhalter für jeden Wert. Für die meisten Gruppen ist dies ein Name in der Form *Eignername*:*Gruppenname*. Einige durch Ihren Systemadministrator erstellte Gruppen besitzen den Präfix *Eignername* nicht. Siehe „Gruppennamen” auf Seite 54.

id Dies ist eine eindeutige Identifikationsnummer, die die AFS-Server-Prozesse intern verwenden. In ihrer Funktion ist sie einer UNIX-UID ähnlich, sie funktioniert jedoch in AFS besser als im UNIX-Dateisystem. Benutzer und Maschinen besitzen positive ganzzahlige AFS-Benutzer-IDs (UIDs), und Gruppen besitzen negative ganzzahlige AFS-Gruppen-IDs (GIDs).

owner Dies ist der Benutzer oder die Gruppe, dem oder der der Eintrag gehört und sie so verwalten kann.

creator
Der Name des Benutzers, der die Befehle **pts createuser** und **pts**

createdgroup eingegeben hat, um den Eintrag zu erstellen. Dieses Feld ist vor allem als Prüfprotokoll nützlich und kann nicht verändert werden.

membership
Für Benutzer und Maschinen zeigt dies an, zu wievielen Gruppen der Benutzer oder die Maschine gehört. Für Gruppen zeigt dies an, wieviele Mitglieder zu dieser Gruppe gehören. Dieser Wert kann nicht explizit eingestellt werden.

flags Dieses Feld zeigt an, wem es gestattet ist, bestimmte Informationen über den Eintrag aufzulisten oder ihn zu verändern. Siehe „Schützen von Gruppeninformationen" auf Seite 65.

group quota
Dieses Feld zeigt an, wie viele weitere Gruppen und Benutzer noch erstellt werden können. Wenn ein Benutzereintrag erstellt wird, ist es auf 20 eingestellt. Die Erstellungsquote für Maschinen oder Gruppen ist bedeutungslos, weil es nicht möglich ist, sich als Maschine oder Gruppe zu authentifizieren.

Beispiel: Auflisten von Informationen über eine Gruppe

Das folgende Beispiel zeigt Informationen über die Gruppe **pat:accounting** an, die aus Mitgliedern der durch **pat** verwalteten Abteilung besteht. Beachten Sie, daß die Gruppe sich selbst gehört, was bedeutet, daß sie durch alle ihre Mitglieder verwaltet werden kann.

```
% pts examine pat:accounting
Name: pat:accounting, id: -673, owner: pat:accounting, creator: pat,
membership: 15, flags: S-M--, group quota: 0
```

Beispiel: Auflisten von Gruppeninformationen über einen Benutzer

Das folgende Beispiel zeigt Gruppeninformationen über den Benutzer **pat** an. Die zwei interessantesten Felder sind membership, das anzeigt, daß **pat** zu 12 Gruppen gehört, und group quota, das anzeigt, daß **pat** 17 neue Gruppen erstellen kann.

```
% pts examine pat
Name: pat, id: 1045, owner: system:administrators, creator: admin,
membership: 12, flags: S-M--, group quota: 17
```

Erstellen von Gruppen und Hinzufügen von Mitgliedern

Verwenden Sie den Befehl **pts creategroup**, um eine Gruppe zu erstellen und den Befehl **pts adduser**, um Mitglieder zu ihr hinzuzufügen. Benutzer und Maschinen können zu Gruppen gehören, andere Gruppen jedoch nicht.

Wenn Sie eine Gruppe erstellen, werden Sie normalerweise automatisch ihr Eigner. Dies bedeutet, Sie können sie allein verwalten: Mitglieder hinzufügen und entfernen, den Gruppennamen ändern, das Eigentumsrecht an der

Gruppe übertragen oder die Gruppe insgesamt löschen. Wenn Sie möchten, können Sie beim Erstellen der Gruppe einen anderen Eigner vorsehen, indem Sie das Argument **-owner** im Befehl **pts creategroup** verwenden. Wenn Sie das Eigentumsrecht einer anderen Gruppe zuweisen, muß die Eignergruppe bereits existieren und mindestens ein Mitglied besitzen. Sie können das Eigentumsrecht einer Gruppe auch nach ihrer Erstellung mit Hilfe des Befehls **pts chown** verändern, wie in „Ändern des Eigners oder des Namens einer Gruppe” auf Seite 63 beschrieben.

So erstellen Sie eine Gruppe

Verwenden Sie den Befehl **pts creategroup**, um eine Gruppe zu erstellen. Ihre Gruppenerstellungsquote sinkt dabei für jede Gruppe um eins.

```
% pts creategroup -name <Gruppenname>+ [-owner <Eigner der Gruppe>]
```

wobei

cg Ist ein Alias für **creategroup** (und **createg** ist kürzeste akzeptable Abkürzung).

-name Bezeichnet jede zu erstellende Gruppe. Der Name muß das folgende Format haben:

Eignername:*Gruppenname*

Das Präfix *Eignername* muß den Eigner der Gruppe exakt angeben. Standardmäßig werden Sie als der Eigner eingesetzt, und *Eignername* muß Ihr AFS-Benutzername sein. Sie können das Argument **-owner** verwenden, um einen anderen AFS-Benutzer oder eine andere AFS-Gruppe zum Eigner zu machen, indem Sie den erforderlichen Wert im Feld *Eignername* eingeben:

- Wenn der Eigner ein Benutzer ist, muß es der AFS-Benutzername sein.
- Wenn der Eigner eine andere reguläre Gruppe ist, muß er mit dem Feld *Eignername* der Eignergruppe übereinstimmen. Wenn, zum Beispiel, die Gruppe **terry:associates** der Eigner ist, muß im Eignerfeld **terry** stehen.
- Wenn der Eigner eine Gruppe ohne Präfix *Eignername* ist, muß es der Name der Eignergruppe sein.

Einschließlich dem Doppelpunkt kann der Name bis zu 63 Zeichen enthalten. Verwenden Sie Ziffern und Kleinbuchstaben, aber keine Leerzeichen und außer dem Doppelpunkt keine Interpunktionszeichen.

-owner

Ist optional und weist das Eigentumsrecht einem anderen Benutzer als Ihnen oder einer Gruppe zu. Wenn Sie eine Gruppe angeben, muß sie bereits existieren und mindestens ein Mitglied besitzen. (Das bedeutet,

daß Sie, erst nachdem Sie mit diesem Befehl die Gruppe erstellt und mit dem Befehl **pts adduser** ein Mitglied hinzugefügt haben, mit dem Befehl **pts chown** der Gruppe selbst das Eigentumsrecht zuweisen können. Siehe „Ändern des Eigners oder des Namens einer Gruppe” auf Seite 63.)

Verwenden Sie keine Maschine als Eigner. Weil sich niemand als Maschine authentifizieren kann, gibt es keine Möglichkeit, eine Gruppe zu verwalten, die einer Maschine gehört.

Beispiel: Erstellen einer Gruppe

Im folgenden Beispiel erstellt Benutzer **terry** eine Gruppe, um alle anderen Benutzer in seinem Team zusammenzufassen, und überprüft dann den neuen Gruppeneintrag.

```
   % pts creategroup terry:team
group terry:team has id -286
% pts examine terry:team
Name: terry:team, id: -286, owner: terry, creator: terry,
membership: 0, flags: S----, group quota: 0.
```

So fügen Sie zu einer Gruppe Mitglieder hinzu

Verwenden Sie den Befehl **pts adduser**, um einen oder mehrere Benutzer zu einer oder mehreren Gruppen hinzuzufügen. Zu ihrer eigenen Gruppe können Sie jederzeit Mitglieder hinzufügen (entweder direkt oder weil Sie zur Eignergruppe gehören). Wenn Sie zu einer Gruppe gehören, können Sie Mitglieder hinzufügen, wenn ihre vierte Zugriffscodemarkierung der Kleinbuchstabe **a** ist; siehe „Schützen von Gruppeninformationen” auf Seite 65.

```
% pts adduser -user <Benutzername>+ -group <Gruppenname>+
```

Wenn es angebracht ist, müssen Sie sich zu Gruppen, die Ihnen gehören, selbst hinzufügen. Sie gehören nicht automatisch dazu, auch wenn Ihnen die Gruppe gehört.

Anmerkung: Wenn Sie bereits ein Token besitzen, während Sie zu einer Gruppe hinzugefügt werden, müssen Sie den Befehl **klog** verwenden, um sich neu zu authentifizieren, bevor Sie die der Gruppe in ACLs erteilten Berechtigungen ausüben können.

wobei

-user Gibt den Benutzernamen jedes Benutzers an, der zu den durch das Argument **-group** bezeichneten Gruppen hinzugefügt werden soll. Gruppen können nicht zu anderen Gruppen gehören.

-group
Bezeichnet jede Gruppe, zu der Benutzer hinzugefügt werden sollen.

Beispiel: Hinzufügen von Mitglieder zu einer Gruppe

In diesem Beispiel fügt Benutzer **terry** sich selbst sowie **pat**, **indira** und **smith** zur gerade erstellten Gruppe **terry:team** hinzu und überprüft dann die neue Mitgliederliste.

```
% pts adduser -user terry pat indira smith -group terry:team
% pts members terry:team
Members of terry:team (id: -286) are:
terry
pat
indira
smith
```

Entfernen von Benutzern aus einer Gruppe und Löschen einer Gruppe

Sie können die folgenden Befehle verwenden, um Gruppen und ihre Mitglieder zu entfernen:

- Um einen Benutzer aus einer Gruppe zu entfernen, verwenden Sie den Befehl **pts removeuser**
- Um eine Gruppe vollständig zu löschen, verwenden Sie den Befehl **pts delete**
- Um gelöschte Gruppen aus ACLs zu entfernen, verwenden Sie den Befehl **fs cleanacl**

Wenn eine von Ihnen erstellte Gruppe gelöscht wird, steigt Ihre Gruppenerstellungsquote um eins, auch wenn Sie nicht mehr der Eigner sind.

Wenn eine Gruppe oder ein Benutzer gelöscht wird, erscheint in den ACLs an der Stelle ihres oder seines AFS-Namens die AFS-ID. Sie können mit dem Befehl **fs cleanacl** diese veralteten Einträge aus den ACLs löschen, für die Sie die Berechtigung **a** (**administer**) besitzen.

So entfernen Sie Mitglieder aus einer Gruppe

Verwenden Sie den Befehl **pts removeuser**, um ein oder mehrere Mitglieder aus einer oder mehreren Gruppen zu entfernen. Aus ihrer eigenen Gruppe können Sie jederzeit Mitglieder entfernen (entweder direkt oder weil Sie zur Eignergruppe gehören). Wenn Sie zu einer Gruppe gehören, können Sie Mitglieder entfernen, wenn ihre fünfte Zugriffscodemarkierung der Kleinbuchstabe **r** ist; siehe „Schützen von Gruppeninformationen” auf Seite 65. (Um sich den Eigner einer Gruppe anzeigen zu lassen, verwenden Sie den Befehl **pts examine**, wie in „So lassen Sie sich einen Gruppeneintrag anzeigen” auf Seite 57 beschrieben.)

```
% pts removeuser -user <Benutzername>+ -group <Gruppenname>+
```

wobei

-user Gibt den Benutzernamen jedes Benutzers an, der aus den durch das Argument **-group** bezeichneten Gruppen entfernt werden soll.

-group
Bezeichnet jede Gruppe, aus der Benutzer entfernt werden sollen.

Beispiel: Entfernen von Gruppenmitgliedern

Das folgende Beispiel entfernt den Benutzer **pat** aus den Gruppen **terry:team** und **terry:friends**.

```
% pts removeuser pat -group terry:team terry:friends
```

So löschen Sie eine Gruppe

Verwenden Sie den Befehl **pts delete**, um eine Gruppe zu löschen. Sie können jederzeit eine Gruppe löschen, die Ihnen gehört (entweder direkt oder weil Sie zur Eignergruppe gehören). Um sich den Eigner einer Gruppe anzeigen zu lassen, verwenden Sie den Befehl **pts examine**, wie in „So lassen Sie sich einen Gruppeneintrag anzeigen" auf Seite 57 beschrieben.

```
% pts delete
<Benutzer oder Gruppenname oder -ID>+
```

wobei *Benutzer oder Gruppenname oder -ID* den Namen oder die AFS-UID jedes Benutzers oder den Namen oder die AFS-GID jeder zu löschenden Gruppe angibt. Beim Identifizieren einer Gruppe über ihre AFS-GID, stellen Sie der GID einen Silbentrennungsstrich (**-**) voran, um anzuzeigen, daß es sich um eine negative Nummer handelt.

Beispiel: Löschen einer Gruppe

Im folgenden Beispiel wird die Gruppe **terry:team** gelöscht.

```
% pts delete terry:team
```

So entfernen Sie veraltete ACL-Einträge

Verwenden Sie den Befehl **fs cleanacl**, um aus ACLs veraltete Einträge zu löschen, nachdem die zugehörigen Benutzer oder Gruppen gelöscht worden sind.

```
% fs cleanacl [<Verzeichnis-/Dateipfad>+]
```

wobei *Verzeichnis-/Dateipfad* der Name jedes Verzeichnisses ist, für das die ACL bereinigt werden soll. Wenn Sie dieses Argument weglassen, wird die ACL des aktuellen Arbeitsverzeichnisses bereinigt.

Beispiel: Entfernen eines veralteten ACL-Eintrags

Nachdem die Gruppe **terry:team** gelöscht wurde, erscheint in den ACLs an der Stelle ihres Namens ihre AFS-GID (-286). In diesem Beispiel entfernt sie Benutzer **terry** aus der ACL im Verzeichnis plans in seinem Ausgangsverzeichnis.

```
% fs listacl plans
Access list for plans is
Normal rights:
terry rlidwka
```

```
-268 rlidwk
sam rliw
% fs cleanacl plans
% fs listacl plans
Access list for plans is
Normal rights:
terry rlidwka
sam rliw
```

Ändern des Eigners oder des Namens einer Gruppe

Um den Eigner einer Gruppe zu ändern, verwenden Sie den Befehl **pts chown**. Um ihren Namen zu ändern, verwenden Sie den Befehl **pts rename**.

Sie können jederzeit den Eigner oder den Namen einer Gruppe ändern, die Ihnen gehört (entweder direkt oder weil Sie zur Eignergruppe gehören). Sie können das Eigentumsrecht an der Gruppe einem anderen Benutzer, einer anderen Gruppe oder der Gruppe selbst zuweisen. Wenn Sie nicht bereits ein Mitglied der Gruppe sind, es aber sein müssen, verwenden Sie den Befehl **pts adduser**, bevor Sie das Eigentumsrecht übertragen, indem Sie die Anweisungen in „So fügen Sie zu einer Gruppe Mitglieder hinzu” auf Seite 60 befolgen.

Der Befehl **pts chown** ändert das Präfix *Eignername* einer Gruppe automatisch und zeigt damit den neuen Eigner an. Wenn der neue Eigner eine Gruppe ist, wird nur Präfix *Eignername* verwendet, und nicht ihr vollständiger Name. Jedoch wird die Änderung im Präfixbefehl *Eignername* nicht an die Gruppen weitergegeben, die der Gruppe gehören, deren Eigner geändert wird. Wenn Sie möchten, daß deren Präfix *Eignername* den richtigen Eigner anzeigt, müssen Sie den Befehl **pts rename** verwenden.

Sonst verwenden Sie den Befehl **pts rename** normalerweise, um nur den Teil *Gruppenname* eines Gruppennamens (der Teil, der dem Doppelpunkt folgt) zu ändern. Sie können das Präfix *Eignername* nur ändern, um den tatsächlichen Eigner widerzuspiegeln.

So ändern Sie den Eigner einer Gruppe

Verwenden Sie den Befehl **pts chown**, um den Eigner einer Gruppe zu ändern.

```
% pts chown  <Gruppenname> <neuer Eigner>
```

wobei

Grupenname
: Gibt den aktuellen Namen der Gruppe an, der ein neuer Eigner zugewiesen werden soll.

neuer Eigner

Bezeichnet den Benutzer oder die Gruppe, dem oder der die Gruppe gehören soll.

Beispiel: Ändern des Eigners einer Gruppe in einen anderen Benutzer

Im folgenden Beispiel überträgt Benutzer **pat** das Eigentumsrecht an der Gruppe **pat:staff** an den Benutzer **terry**. Ihr Name ändert sich automatisch in **terry:staff**, wie es durch den Befehl **pts examine** bestätigt wird.

```
% pts chown pat:staff terry
% pts examine terry:staff
Name: terry:staff, id: -534, owner: terry, creator: pat,
membership: 15, flags: SOm--, group quota: 0.
```

Beispiel: Ändern des Eigners einer Gruppe in die Gruppe selbst

Im folgenden Beispiel macht **terry** die Gruppe **terry:team** zu einer sich selbst gehörenden Gruppe. Ihr Name ändert sich nicht, weil ihr Präfix *Eignername* bereits **terry** ist.

```
% pts chown terry:team terry:team
% pts examine terry:team
Name: terry:team, id: -286, owner: terry:team, creator: terry,
membership: 6, flags: SOm--, group quota: 0.
```

Beispiel: Ändern des Eigners einer Gruppe in eine Gruppe

In diesem Beispiel überträgt Benutzer **sam** das Eigentumsrecht an der Gruppe **sam:project** an die Gruppe **smith:cpa**. Ihr Name ändert sich automatisch in **smith:project**, weil **smith** das Präfix *Eignername* der neuen Eignergruppe ist. Der Befehl **pts examine** zeigt den Status der Gruppe vor und nach der Änderung an.

```
% pts examine sam:project
Name: sam:project, id: -522, owner: sam, creator: sam,
membership: 33, flags: SOm--, group quota: 0.
% pts chown sam:project smith:cpa
% pts examine smith:project
Name: smith:project, id: -522, owner: smith:cpa, creator: sam,
membership: 33, flags: SOm--, group quota: 0.
```

So ändern Sie den Namen einer Gruppe

Verwenden Sie den Befehl **pts rename**, um den Namen einer Gruppe zu ändern.

```
% pts rename  <alter Name> <neuer Name>
```

wobei

alter Name

Gibt den aktuellen Namen der Gruppe an.

neuer Name

Gibt den vollständigen neuen Namen an, der der Gruppe zugewiesen werden soll. Das Präfix *Eignername* muß den Eigner der Gruppe exakt angeben.

Beispiel: Ändern des Suffixes *Gruppenname* einer Gruppe

Das folgende Beispiel ändert den Namen der Gruppe **smith:project** in **smith:fiscal-closing**. Das Präfix *Eignername* der Gruppe bleibt **smith**, weil der Eigner nicht gewechselt hat.

```
% pts examine smith:project
Name: smith:project, id: -522, owner: smith:cpa, creator: sam,
membership: 33, flags: SOm--, group quota: 0.
% pts rename smith:project smith:fiscal-closing
% pts examine smith:fiscal-closing
Name: smith:fiscal-closing, id: -522, owner: smith:cpa, creator: sam,
membership: 33, flags: SOm--, group quota: 0.
```

Beispiel: Ändern des Präfixes *Eignername* einer Gruppe

In einem vorherigen Beispiel übertrug Benutzer **pat** das Eigentumsrecht an der Gruppe **pat:staff** an den Benutzer **terry**. Ihr Name wurde automatisch in **terry:staff** geändert. Jedoch ist eine Gruppe, die **terry:staff** gehört, noch mit **pat:plans** bezeichnet, weil die Änderung des *Eignername* einer Gruppe im Ergebnis des Befehls **pts chown** nicht an die anderen Gruppen, die ihr gehören, weitergegeben wurde. In diesem Beispiel verwendet ein Mitglied von **terry:staff** den Befehl **pts rename**, um den Namen in **terry:plans** zu ändern und damit ihr Eigentumsrecht widerzuspiegeln.

```
% pts examine pat:plans
Name: pat:plans, id: -535, owner: terry:staff, creator: pat,
membership: 8, flags: SOm--, group quota: 0.
% pts rename pat:plans terry:plans
% pts examine terry:plans
Name: terry:plans, id: -535, owner: terry:staff, creator: pat,
membership: 8, flags: SOm--, group quota: 0.
```

Schützen von Gruppeninformationen

Die *Zugriffscodemarkierungen* einer Gruppe steuern, wer die Gruppe auf welche Weise verwalten kann. Die Zugriffscodemarkierungen erscheinen im Feld `flags` der Ausgabe des Befehls **pts examine**; siehe „So lassen Sie sich einen Gruppeneintrag anzeigen” auf Seite 57. Um die Zugriffscodemarkierungen für eine Ihnen gehörende Gruppe einzustellen, verwenden Sie den Befehl **pts setfields**, wie in „So stellen Sie die Zugriffscodemarkierungen einer Gruppe ein” auf Seite 66 beschrieben.

Interpretieren der Zugriffscodemarkierungen

Die fünf Zugriffscodemarkierungen erscheinen immer und müssen immer in der folgenden Reihenfolge eingestellt werden:

s Steuert, wer den Befehl **pts examine** verwenden kann, um den Eintrag anzuzeigen.

o Steuert, wer den Befehl **pts listowned** verwenden kann, um sich die Gruppen anzeigen zu lassen, die einem Benutzer oder einer Gruppe gehören.

m Steuert, wer den Befehl **pts membership** verwenden kann, um sich die Gruppen anzeigen zu lassen, zu denen ein Benutzer oder eine Maschine gehört, oder um sich anzeigen zu lassen, welche Benutzer oder Maschinen zu einer Gruppe gehören.

a Steuert, wer den Befehl **pts adduser** verwenden kann, um einen Benutzer oder eine Maschine zu einer Gruppe hinzuzufügen.

r Steuert, wer den Befehl **pts removeuser** verwenden kann, um einen Benutzer oder eine Maschine aus einer Gruppe zu entfernen.

Jede Markierung kann Werte dreier möglicher Typen annehmen, um es einer anderen Benutzergruppe zu ermöglichen, den zugehörigen Befehl zu verwenden:

- Ein Silbentrennungsstrich (-) bedeutet, daß der Eigner der Gruppe den Befehl gemeinsam mit den Administratoren verwenden kann, die zu Gruppe **system:administrators** gehören.
- Der Kleinbuchstabe bedeutet, daß die Mitglieder der Gruppe den Befehl verwenden können, wie auch die Benutzer, die durch den Silbentrennungsstrich angezeigt werden.
- Der Großbuchstabe bedeutet, daß jeder den Befehl verwenden kann.

Zum Beispiel zeigen die Markierungen `SOmar` zu einem Gruppeneintrag an, daß jeder den Eintrag der Gruppe überprüfen und die Gruppen, die ihr gehören, auflisten kann, und daß nur die Mitglieder der Gruppe Mitglieder auflisten, hinzufügen oder entfernen können.

Die Standardeinstellungen der Zugriffscodemarkierungen für Gruppen sind `S-M--`, was bedeutet, daß sich jeder den Eintrag anzeigen und die Mitglieder der Gruppe auflisten lassen kann, daß aber nur der Eigner der Gruppe und die Mitglieder der Gruppe **system:administrators** andere Funktionen ausführen können.

So stellen Sie die Zugriffscodemarkierungen einer Gruppe ein

Verwenden Sie den Befehl **pts setfields**, um die Zugriffscodemarkierungen für eine oder mehrere Gruppen einzustellen.

```
% pts setfields -nameorid <Benutzer oder Gruppenname oder -ID>+
-access <Zugriffscodemarkierungen festlegen>
```

wobei

-nameorid

Gibt den Namen oder die AFS-GID jeder Gruppe an, für die die Zugriffscodemarkierungen eingestellt werden sollen. Beim Identifizieren einer Gruppe über ihre AFS-GID, stellen Sie der GID einen Silbentrennungsstrich (**-**) voran, um anzuzeigen, daß es sich um eine negative Nummer handelt.

-access

Gibt die für jede Gruppe einzustellenden Zugriffscodemarkierungen an. Beachten Sie die folgenden Regeln:

- Geben Sie für alle fünf Markierungen Werte in der Reihenfolge **somar** ein.
- Verwenden Sie für die erste Markierung ausschließlich den Kleinbuchstaben **s** oder den Großbuchstaben **S**.
- Verwenden Sie für die zweite Markierung ausschließlich den Silbentrennungsstrich (**-**) oder den Großbuchstaben **O**. Für Gruppen interpretiert AFS den Silbentrennungsstrich als Kleinbuchstaben **o** (das heißt, Mitglieder einer Gruppe können stets die der Gruppe gehörenden Gruppen auflisten).
- Verwenden Sie für die dritte Markierung den Silbentrennungsstrich (**-**), den Kleinbuchstaben **m** oder den Großbuchstaben **M**.
- Verwenden Sie für die vierte Markierung den Silbentrennungsstrich (**-**), den Kleinbuchstaben **a** oder den Großbuchstaben **A**. Der Großbuchstabe **A** ist keine sichere Wahl, weil es damit jedem gestattet ist, Mitglieder zur Gruppe hinzuzufügen.
- Verwenden Sie für die fünfte Markierung ausschließlich den Silbentrennungsstrich (**-**) oder den Kleinbuchstaben **r**.

Beispiel: Einstellen der Zugriffscodemarkierungen einer Gruppe

Das folgende Beispiel stellt die Zugriffscodemarkierungen für die Gruppe **terry:team** ein, um das angegebene Muster von Verwaltungsberechtigungen zu realisieren.

```
% pts setfields terry:team -access SOm--
```

- Jeder kann den Befehl **pts examine** verwenden, um sich Basisinformationen zur Gruppe anzeigen zu lassen (Großbuchstabe **S**).
- Jeder kann den Befehl **pts listowned** verwenden, um sich die der Gruppe gehörenden Gruppen anzeigen zu lassen (Großbuchstabe **O**).
- Die Mitglieder der Gruppe können den Befehl **pts membership** verwenden, um sich die Mitglieder der Gruppe anzeigen zu lassen (Kleinbuchstabe **m**).
- Nur der Eigner der Gruppe, Benutzer **terry**, kann den Befehl **pts adduser** verwenden, um Mitglieder hinzuzufügen (der Silbentrennungsstrich).
- Nur der Eigner der Gruppe, Benutzer **terry**, kann den Befehl **pts removeuser** verwenden, um Mitglieder zu entfernen (der Silbentrennungsstrich).

Kapitel 6. Fehlerbehebung

In diesem Kapitel wird beschrieben, wie bestimmte Fehler festgestellt und behoben werden, die beim Arbeiten mit AFS-Dateien manchmal auftreten können. Suchen Sie zuerst die Überschrift, die den aufgetretenen Fehler beschreibt oder die emittierte Fehlernachricht zitiert. Gehen Sie dann anhand der Anweisungen vor.

Fehler: Zugriff auf Datei kann nicht durchgeführt oder Datei kann nicht kopiert oder gespeichert werden

1. Führen Sie den Befehl **tokens** aus, um sicherzustellen, daß Sie über gültige Token verfügen. Vollständige Anweisungen hierzu enthält der Abschnitt „So lassen Sie sich Ihre Token anzeigen" auf Seite 17.

   ```
   % tokens
   ```

   - Wenn Ihre Token gültig sind, fahren Sie mit Schritt 2 fort.
   - Wenn keine Token für die relevante Zelle vorliegen oder diese abgelaufen sind, führen Sie den Befehl **klog** zur Authentifizierung aus. Vollständige Anweisungen hierzu enthält der Abschnitt „So authentifizieren Sie sich bei AFS" auf Seite 16. Versuchen Sie den Zugriff auf die Datei oder das Speichern der Datei dann erneut. Wenn der Vorgang nach wie vor nicht erfolgreich durchgeführt werden kann, fahren Sie mit Schritt 2 fort.

     ```
     % klog
     ```

2. Führen Sie den Befehl **fs checkservers** aus, um den Status der Datei-Server-Maschinen zu überprüfen. Vollständige Anweisungen hierzu enthält der Abschnitt „Prüfen des Status von Server-Maschinen" auf Seite 29.

   ```
   % fs checkservers &
   ```

   - Wenn die folgende Nachricht angezeigt wird, fahren Sie mit Schritt 3 auf Seite 70 fort.

     ```
     All servers are running.
     ```

   - Eine Ausgabe ähnlich der im folgenden angegebenen Ausgabe weist darauf hin, daß der Cache Manager keine Verbindung zu den angegebenen Datei-Server-Maschinen herstellen kann.

     ```
     These servers unavailable due to network or server problem:
     list of machines.
     ```

     Führen Sie den Befehl **fs whereis** aus, um zu überprüfen, ob sich die Datei, auf die zugegriffen oder die gespeichert werden soll, auf einer der Datei-Server-Maschinen befindet, auf die nicht zugegriffen werden kann. Vollständige Anweisungen hierzu enthält der Abschnitt „Suchen von Dateien und Verzeichnissen" auf Seite 28.

© Copyright IBM Corp. 1989, 2000

```
% fs whereis <Verzeichnis-/Dateipfad>
```

Wenn die Datei auf einer Maschine gespeichert ist, auf die nicht zugegriffen werden kann, können Sie nicht auf die Datei zugreifen, oder sie auf dem Datei-Server speichern, bis der Zugriff auf die Maschine wieder möglich ist. Wenn sich die Datei auf einer Maschine befindet, die nicht in der Liste der Maschinen aufgeführt ist, auf die kein Zugriff möglich ist, fahren Sie mit Schritt 3 fort.

3. Führen Sie den Befehl **fs listacl** aus, um sicherzustellen, daß Sie über die erforderlichen Berechtigungen verfügen, um auf die Datei zugreifen, die Datei kopieren oder speichern zu können. Vollständige Anweisungen hierzu enthält der Abschnitt „Vorgehensweise beim Anzeigen einer ACL” auf Seite 40.

   ```
   % fs listacl <Verzeichnis-/Dateipfad>
   ```

   Sie müssen über die angegebenen Berechtigungen verfügen:

   - Damit Sie auf eine Datei zugreifen, eine Datei kopieren oder speichern können, müssen Sie über die **l** (**lookup**)-Berechtigung für das Verzeichnis und für alle übergeordneten Verzeichnisse im Pfadnamen verfügen.
   - Damit Sie Änderungen in eine vorhandene Datei speichern können, müssen Sie zusätzlich dazu über die **w** (**write**)-Berechtigung verfügen. Damit Sie eine neue Datei erstellen können, müssen Sie zusätzlich dazu über die Berechtigungen **i** (**insert**) und **w** verfügen.
   - Damit Sie eine Datei von einem Verzeichnis in ein anderes kopieren können, müssen Sie zusätzlich dazu über die **r** (**read**)-Berechtigung für das Quellenverzeichnis und über die **i**-Berechtigung für das Zielverzeichnis verfügen.

   Wenn Sie nicht über die erforderlichen Berechtigungen verfügen, jedoch Eigner des Verzeichnisses sind, verfügen Sie stets über die **a** (**administer**)-Berechtigung, selbst wenn Sie nicht in der ACL aufgeführt sind. Führen Sie den Befehl **fs setacl** aus, um sich selbst die erforderlichen Berechtigungen zu erteilen. Vollständige Anweisungen hierzu enthält der Abschnitt „Ändern einer ACL” auf Seite 42.

   ```
   % fs setacl  -dir <Verzeichnis>+ -acl <Zugriffslisteneinträge>+
   ```

   Wenn Sie nicht über die erforderlichen Berechtigungen verfügen und nicht Eigner des Verzeichnisses sind, bitten Sie den Eigner oder einen Systemadministrator darum, Ihnen die entsprechenden Berechtigungen zu erteilen. Wenn der Eigner oder der Systemadministrator Sie einer Gruppe hinzufügt, die über die erforderlichen Berechtigungen verfügt, müssen Sie den Befehl **klog** für eine erneute Authentifizierung ausführen, bevor Sie mit den Berechtigungen arbeiten können.

Wenn Sie trotz vorliegender erforderlicher Berechtigungen immer noch nicht auf die Datei zugreifen können, besprechen Sie das Problem mit dem Systemadministrator, um weitere mögliche Ursachen des Problems zu untersuchen. Wenn Sie trotz vorliegender erforderlicher Berechtigungen die Datei immer noch nicht kopieren oder speichern können, fahren Sie mit Schritt 4 fort.

4. Führen Sie beim Kopieren einer Datei den Befehl **fs listquota** aus, um zu überprüfen, ob das Volume, in das die Datei kopiert wird, oder die Partition, auf der sich das Volume befindet, fast vollständig belegt ist. Überprüfen Sie beim Speichern einer Datei das Volume und die Partition, die das Verzeichnis enthalten, in dem die Datei gespeichert wird. Vollständige Anweisungen hierzu enthält der Abschnitt „Anzeigen der Quote eines Volumes” auf Seite 25.

   ```
   % fs listquota <Verzeichnis-/Dateipfad>
   ```

   Mit dem Befehl wird eine Ausgabe produziert, die ähnlich wie das folgende Ausgabenbeispiel aussieht:

   ```
   % fs listquota /afs/abc.com/usr/terry
   Volume Name     Quota    Used    % Used   Partition
   user.terry      10000    3400       34%         86%
   ```

   - Wenn der Wert im Feld `Partition` nicht nahe 100% ist, ist die Partition nicht nahezu vollständig belegt. Prüfen Sie den Wert im Feld `% Used`. Wenn dieser Wert nahe 100% ist, ist das Volume nahezu vollständig belegt. Löschen Sie in dem Fall, wenn möglich, Dateien aus dem Volume, die nicht mehr benötigt werden, oder bitten Sie den Systemadministrator darum, die Quote des Volumes zu erhöhen.

     Wenn der Wert im Feld `% Used` nicht nahe 100% ist (wenn er z.B. 90% oder weniger beträgt), dann ist es unwahrscheinlich, daß Sie die Quote des Volumes überschreiten, es sei denn, die Datei ist sehr groß oder die Quote des Volumes ist klein. Besprechen Sie das Problem mit dem Systemadministrator, um weitere mögliche Ursachen des Problems zu untersuchen.

   - Wenn der Wert im Feld `Partition` sehr nahe 100% ist, ist die Partition wahrscheinlich nahezu vollständig belegt. Partitionen von Server-Maschinen sind in der Regel jedoch sehr groß und können immer noch über ausreichend Speicherplatz für eine Datei durchschnittlicher Größe verfügen, auch wenn sie nahezu vollständig belegt sind. Sie können entweder Ihren Systemadministrator zum Partitionsstatus befragen oder den Befehl **fs examine** ausführen. In der letzten Zeile der Ausgabe des Befehls wird angegeben, wie viele Kilobyteblöcke auf der Partition noch zur Verfügung stehen. Vollständige Anweisungen hierzu enthält der Abschnitt „Anzeigen der Quote eines Volumes” auf Seite 25.

     ```
     % fs examine <Verzeichnis-/Dateipfad>
     ```

Wenn auf der Partition ausreichend freier Speicherbereich vorhanden ist, Sie die Datei aber noch immer nicht speichern können, besprechen Sie das Problem mit dem Systemadministrator, um weitere mögliche Ursachen des Problems zu untersuchen.

Problem: Eigener Eintrag wurde versehentlich aus einer ACL entfernt

1. Wenn Sie Eigner des Verzeichnisses sind, aus dem Sie den ACL-Eintrag versehentlich entfernt haben, verfügen Sie immer noch über die **a** (**administer**)-Berechtigung, selbst wenn dies nicht in der ACL aufgeführt ist. Normalerweise sind Sie Eigner Ihres Ausgangsverzeichnisses und dessen gesamter Unterverzeichnisse. Führen Sie den Befehl **fs setacl** aus, um sich selbst alle anderen Berechtigungen zu erteilen. Vollständige Anweisungen hierzu enthält der Abschnitt „Hinzufügen, Entfernen oder Editieren normaler ACL-Berechtigungen” auf Seite 43.

   ```
   % fs setacl  -dir <Verzeichnis> -acl <Ihr_Benutzername> all
   ```

   Geben Sie für *Verzeichnis* den vollständigen Pfadnamen für das Verzeichnis an (zum Beispiel **/afs/abc.com/usr/***Ihr_Benutzername*). Dies ist erforderlich, da AFS Abkürzungen von Pfadnamen nicht interpretieren kann, wenn Sie nicht über die **l** (**lookup**)-Berechtigung verfügen.

2. Wenn Sie nicht Eigner des Verzeichnisses sind, führen Sie den Befehl **fs listacl** aus, um zu überprüfen, ob Ihnen über restliche Einträge die erforderlichen Berechtigungen erteilt wurden (möglicherweise gehören Sie zu einer oder zu mehreren Gruppen, die in der ACL aufgeführt werden). Vollständige Anweisungen hierzu enthält der Abschnitt „Vorgehensweise beim Anzeigen einer ACL” auf Seite 40.

   ```
   % fs listacl <Verzeichnis-/Dateipfad>
   ```

   - In der folgenden Nachricht wird die ACL des Verzeichnisses angegeben. Wenn Sie Berechtigungen benötigen, die Sie derzeit über keinen der Einträge erteilt bekommen, bitten Sie den Eigner des Verzeichnisses oder den Systemadministrator um Hilfe.

     ```
     Access list for <Verzeichnis-/Dateipfad> is
     Normal rights
     list of entries
     ```

   - Wenn der Befehl anstelle einer ACL die folgende Fehlernachricht zurückgibt, verfügen Sie nicht über die **l**-Berechtigung.

     ```
     fs: You don't have the required access rights on 'dir/file path'
     ```

     Bitten Sie den Verzeichniseigner oder den Systemadministrator darum, Ihnen die erforderlichen Berechtigungen zu erteilen. Wenn der Eigner oder der Systemadministrator Sie einer Gruppe hinzufügt, die über die erforderlichen Berechtigungen verfügt, müssen Sie den Befehl **klog** für eine erneute Authentifizierung ausführen, bevor Sie mit den Berechtigungen arbeiten können.

Fehlernachricht: ″afs: Lost contact with fileserver″

Führen Sie den Befehl **fs checkservers** aus, um den Status der Datei-Server-Maschinen zu überprüfen. Vollständige Anweisungen hierzu enthält der Abschnitt „Prüfen des Status von Server-Maschinen” auf Seite 29.

```
% fs checkservers &
```

- Wenn die folgende Nachricht emittiert wird, bitten Sie den Systemadministrator um Unterstützung bei der Diagnose der Ursache der Fehlernachricht `Lost contact`.

  ```
  All servers are running.
  ```

- Eine Ausgabe, die wie die folgende Ausgabe aussieht, weist darauf hin, daß der Cache Manager keine Verbindung zu den angegebenen Datei-Server-Maschinen herstellen kann. Sie müssen so lange warten, bis wieder auf die Datei-Server-Maschinen zugegriffen werden kann, bevor Sie weiter mit den Dateien arbeiten können, die auf den Servern gespeichert sind.

  ```
  These servers unavailable due to network or server problem:
  Liste_der_Maschinen.
  ```

Fehlernachricht: ″*Command*: Connection timed out″

Führen Sie den Befehl **fs checkservers** aus, wie unter „Fehlernachricht: ″afs: Lost contact with fileserver″” beschrieben.

Fehlernachricht: ″ fs: You don’t have the required access rights on ’*Datei*’″

Sie verfügen nicht über die ACL-Berechtigungen, die erforderlich sind, um die versuchte Operation ausführen zu können. Wenn Sie Eigner des Verzeichnisses sind und Ihren eigenen Eintrag versehentlich aus der ACL entfernt haben, lesen Sie die Informationen unter „Problem: Eigener Eintrag wurde versehentlich aus einer ACL entfernt” auf Seite 72. Andernfalls bitten Sie den Verzeichniseigner oder den Systemadministrator darum, Ihnen die erforderlichen Berechtigungen zu erteilen.

Fehlernachricht: ″afs: failed to store file″

Befolgen Sie die Anweisungen unter „Fehler: Zugriff auf Datei kann nicht durchgeführt oder Datei kann nicht kopiert oder gespeichert werden” auf Seite 69.

Anhang A. Verwenden des NFS/AFS Translator

Einige Zellen verwenden zusätzlich zu AFS das Network File System (NFS). Wenn Sie an einer NFS-Client-Maschine arbeiten, kann der Systemadministrator diese so konfigurieren, daß der Zugriff auf den AFS-Dateibereich über das Programm *NFS/AFS Translator* erfolgt. Wenn Sie über einen AFS-Benutzereintrag verfügen, können Sie als authentifizierter Benutzer von einer NFS-Client-Maschine aus auf AFS zugreifen. Andernfalls greifen Sie auf AFS als Benutzer **anonymous** zu.

Anmerkung: Um eine akzeptable Leistung des NFS / AFS Translator zu gewährleisten, ist es erforderlich, daß NFS korrekt funktioniert.

Voraussetzungen für die Verwendung des NFS/AFS Translator

Damit Sie den NFS / AFS Translator verwenden können, muß der Systemadministrator die folgenden Typen der Maschinen wie angegeben konfigurieren:

- Eine *NFS/AFS Translator-Maschine* ist eine AFS-Client-Maschine, die auch als NFS-Server-Maschine fungiert. Der Cache Manager agiert als der Ersatz-Cache Manager für die NFS-Client-Maschine. Befragen Sie Ihren Systemadministrator dazu, welche Translator-Maschinen Sie verwenden können.
- Die NFS-Client-Maschine muß über einen NFS-Mount zu einer Translator-Maschine verfügen. Meistens hängt der Systemadministrator das Verzeichnis **/afs** der Translator-Maschine an und benennt den Mount auch als **/afs**. Dies ermöglicht es Ihnen, unter Verwendung von Standard-AFS-Pfadnamen auf den gesamten AFS-Dateibereich zuzugreifen. Es ist auch möglich, Mounts direkt für Unterverzeichnisse von **/afs** zu erstellen und NFS-Mounts an der NFS-Client-Maschine verschiedene Namen zu geben.

Der Zugriff auf AFS ist umfassender, wenn Sie über einen AFS-Benutzereintrag verfügen. Wenn dies nicht der Fall ist, erkennen Sie die AFS-Server als Benutzer **anonymous** und erteilen Ihnen nur den Zugriff, der Mitgliedern der Gruppe **system:anyuser** zur Verfügung steht.

Wenn die NFS-Client-Maschine ein Betriebssystem verwendet, das von AFS unterstützt wird, kann der Systemadministrator diese so konfigurieren, daß Sie viele AFS-Befehle auf der Maschine absetzen können. Befragen Sie den Systemadministrator zu der Konfiguration und dazu, welche Befehle abgesetzt werden können.

© Copyright IBM Corp. 1989, 2000

Zugriff auf AFS über den Translator

Wenn Sie über keinen AFS-Benutzereintrag verfügen oder nicht als authentifizierter Benutzer auf AFS zugreifen möchten, dann ist alles, was Sie für den Zugriff auf AFS tun müssen, die Angabe des Pfadnamens der entsprechenden Datei. Die zugehörige ACL muß die erforderlichen Berechtigungen für die Gruppe **system:anyuser** erteilen.

Wenn Sie über einen AFS-Benutzereintrag verfügen und auf AFS als authentifizierter Benutzer zugreifen möchten, hängt die beste Methode davon ab, ob die NFS-Maschine ein unterstützter Typ ist. Wenn dies der Fall ist, gehen Sie nach den Anweisungen unter „Authentifizieren auf einem unterstützten Betriebssystem" vor. Wenn dies nicht der Fall ist, gehen Sie nach den Anweisungen unter „Authentifizieren auf einem nicht unterstützten Betriebssystem" vor.

Authentifizieren auf einem unterstützten Betriebssystem

1. Melden Sie sich an der NFS-Client-Maschine unter Verwendung Ihres NFS-Benutzernamens an.
2. Führen Sie den Befehl **klog** aus. Vollständige Anweisungen hierzu enthält der Abschnitt „So authentifizieren Sie sich bei AFS" auf Seite 16.

   ```
   % klog -setpag
   ```

Authentifizieren auf einem nicht unterstützten Betriebssystem

1. Melden Sie sich an der NFS-Client-Maschine unter Verwendung Ihres NFS-Benutzernamens an.
2. Stellen Sie eine Verbindung mit der NFS/AFS Translator-Maschine her, die Sie verwenden (zum Beispiel unter Verwendung des Dienstprogramms **Telnet**), und melden Sie sich an ihr mit Ihrem AFS-Benutzernamen an (dieser stimmt normalerweise mit Ihrem NFS-Benutzernamen überein).
3. Wenn die NFS/AFS Translator-Maschine ein für AFS angepaßtes Anmeldedienstprogramm verwendet, dann haben Sie in Schritt 2 AFS-Token erhalten. Um dies zu überprüfen, führen Sie den Befehl **tokens** aus, der unter „So lassen Sie sich Ihre Token anzeigen" auf Seite 17 ausführlich beschrieben wird.

   ```
   % tokens
   ```

   Wenn Sie über keine Token verfügen, führen Sie den Befehl **klog** aus, der unter „So authentifizieren Sie sich bei AFS" auf Seite 16 ausführlich beschrieben wird.

   ```
   % klog -setpag
   ```

4. Führen Sie den Befehl **knfs** aus, um die AFS-Token der UNIX-UID auf der NFS-Client-Maschine zuzuordnen, an der Sie arbeiten. Dies ermöglicht es dem Cache Manager auf der Translator-Maschine, die Token beim Zugriff auf AFS von der NFS-Client-Maschine aus ordnungsgemäß zu verwenden.

Wenn die NFS-Client-Maschine ein Systemtyp ist, für den AFS einen Systemnamen definiert, kann es sinnvoll sein, das Argument **-sysname** hinzuzufügen. Dieses Argument unterstützt den Cache Manager beim Zugriff auf für die NFS-Client-Maschine spezifischen Binärdateien, wenn der Systemadministrator die Variable *@sys* in Pfadnamen verwendet hat. Befragen Sie den Systemadministrator dazu, ob dieses Argument für Sie nützlich ist.

```
% knfs <Host-Name> [<Benutzer-ID (dezimal)>]  \
       [-sysname <'@sys'-Wert d. Hosts>]
```

Dabei gilt folgendes:

Host-Name
: gibt den vollständig qualifizierten Host-Namen der NFS-Client-Maschine an (wie z.B. **nfs52.abc.com**).

Benutzer-ID
: gibt Ihre UNIX-UID oder äquivalente ID (nicht Ihren Benutzernamen) auf der NFS-Client-Maschine an. Wenn der Systemadministrator konventionell vorgegangen ist, sind Ihre UNIX- und AFS-UIDs identisch. Wenn Ihnen Ihre lokale UID auf der NFS-Maschine nicht bekannt ist, fragen Sie den Systemadministrator danach. Der Systemadministrator kann auch die Punkte erläutern, auf die Sie achten müssen, wenn Ihre beiden UIDs nicht übereinstimmen, oder wenn Sie dieses Argument weglassen.

-sysname
: gibt den Namen des Systemtyps der NFS-Client-Maschine an.

5. (**Optional**) Melden Sie sich von der Translator-Maschine ab, aber führen Sie keine Deauthentifizierung durch.
6. Arbeiten Sie an der NFS-Client-Maschine, und greifen Sie, falls erforderlich, auf AFS zu.
7. Wenn Sie den Zugriff auf AFS beendet haben, führen Sie erneut den Befehl **knfs** auf der Translator-Maschine aus. Geben Sie dieselben Werte für die Argumente *Host-Name* und *Benutzer-ID* wie in Schritt 4 auf Seite 76 an, und fügen Sie die Markierung **-unlog** hinzu, um die Token zu zerstören. Wenn Sie sich in Schritt 5 von der Translator-Maschine abgemeldet hatten, müssen Sie zuerst die Verbindung mit der Translator-Maschine wiederherstellen (siehe Schritt 2 auf Seite 76).

   ```
   % knfs <Host-Name> [<Benutzer-ID (dezimal)>] -unlog
   ```

Fehlerbehebung für den NFS/AFS Translator

Ob die Leistung des NFS/AFS Translator akzeptabel ist, hängt überwiegend vom NFS ab. Manchmal werden Probleme, die vordergründig nach Ausfällen des AFS-Datei-Servers aussehen, wie z.B. Unterbrechungen von Verbindungen oder Dateien, auf die nicht zugegriffen werden kann, durch NFS-Ausfälle verursacht.

In diesem Abschnitt werden einige häufig auftretende Probleme und deren mögliche Ursachen beschrieben. Wenn andere Probleme auftreten, wenden Sie sich an den Systemadministrator. Dieser kann gegebenenfalls die Gruppe für AFS-Produktunterstützung um Hilfe bitten.

Anmerkung: Um eine Verschlechterung der AFS-Leistung zu verhindern, sendet der Cache Manager an der Translator-Maschine Änderungen, die an den NFS-Client-Maschinen vorgenommen wurden, nicht sofort an den File Server. Statt dessen prüft der Cache Manager im Abstand von 60 Sekunden, ob derartige Änderungen vorliegen, und sendet diese dann. Das Sichern von Änderungen, die an einer NFS-Client-Maschine vorgenommen wurden, kann länger dauern als das Sichern von Änderungen, die an einer AFS-Client-Maschine vorgenommen wurden. Die Sicherungsoperation muß beendet sein, bevor die Änderungen auf NFS-Client-Maschinen, die eine andere Translator-Maschine verwenden, oder auf AFS-Client-Maschinen sichtbar sind.

NFS-Client-Maschine ist im Zustand "Frozen"

Wenn der Systemadministrator die empfohlenen Optionen beim Erstellen eines NFS-Mounts zu einer NFS/AFS-Translator-Maschine verwendet hat, ist der Mount sowohl *hard* als auch *interruptible*:

- Ein Hard-Mount bedeutet, daß der NFS-Client seine Anforderungen wiederholt, wenn er innerhalb des erwarteten Zeitrahmens keine Antwort empfängt. Dies ist von Vorteil, da Anforderungen sowohl die NFS- als auch durch die AFS-Client-Software durchlaufen müssen. Dies kann manchmal länger dauern, als es der NFS-Client erwartet. Dies bedeutet jedoch, daß, wenn tatsächlich kein Zugriff auf die NFS/AFS-Translator-Maschine möglich ist, die NFS-Client-Maschine in einen funktionsunfähigen Status übergehen kann (Status *freeze* oder *hang*).
- Wenn der NFS-Mount interruptible ist, können Sie im Falle eines Ausfalls einer NFS/AFS-Translator-Maschine die Tasten <**Ctrl-C**> drücken oder ein anderes Unterbrechungssignal absetzen, um die wiederholten Versuche des NFS-Clients, auf das AFS zuzugreifen, anzuhalten. Sie können dann lokal mit der Arbeit fortfahren oder einen NFS-Mount zu einer anderen Translator-Maschine erstellen. Wenn der NFS-Mount nicht unterbrechbar ist, müssen Sie den Mount auf die Translator-Maschine, auf die nicht zugegriffen werden kann, explizit entfernen.

Warmstart des NFS/AFS Translator

Wenn Sie eine Authentifizierung für AFS vorgenommen haben und die Translator-Maschine einen Warmstart durchführt, müssen Sie den Befehl **klog** (und gegebenenfalls den Befehl **knfs**) zur erneuten Authentifizierung ausführen. Wenn Sie das Argument **-sysname** des Befehls **knfs** verwendeten, um den Systemnamen der NFS-Client-Maschine zu definieren, verwenden Sie ihn wieder.

Systemfehlernachrichten

In diesem Abschnitt werden die möglichen Bedeutungen von NFS-Fehlernachrichten erläutert, die Sie beim Zugriff auf den AFS-Dateibereich empfangen.

```
stale NFS client
```

```
Getpwd: can't read
```

Beide Nachrichten weisen möglicherweise darauf hin, daß ein Warmstart für die Translator-Maschine durchgeführt wurde und der Pfadname für das aktuelle Arbeitsverzeichnis nicht festgestellt werden konnte. Ändern Sie zum Wiederherstellen des Pfads das Verzeichnis, und geben Sie den vollständigen Pfadnamen beginnend mit **/afs** an.

NFS server *Translator_Maschine* is not responding still trying.

Der NFS-Client empfängt keine Antwort von der NFS/AFS-Translator-Maschine. Wenn es sich bei dem NFS-Mount zur Translator-Maschine um einen absoluten Mount handelt, fährt der NFS-Client damit fort, die Anforderung zu wiederholen, bis er eine Antwort empfängt (siehe „NFS-Client-Maschine ist im Zustand ″Frozen″” auf Seite 78). Wenn es sich bei dem NFS-Mount zur Translator-Maschine um einen bedingten Mount handelt, stoppt der NFS-Client die Wiederholungsversuche nach einer bestimmten Anzahl von Versuchen (standardmäßig drei).

Anhang B. AFS-Befehlssyntax und Online-Hilfefunktion

Die AFS-Befehle, die Ihnen zur Verfügung stehen, werden zur Authentifizierung zum Auflisten von AFS-Informationen, für den Zugriffsschutz von Verzeichnissen, zum Erstellen und Verwalten von Gruppen und zum Erstellen und Verwalten von ACLs verwendet. Es gibt drei allgemeine Befehlsgruppen, die allen AFS-Benutzern zur Verfügung stehen: Datei-Server-Befehle, Zugriffsschutz-Server-Befehle und die Gruppe mit sonstigen Befehlen. In diesem Kapitel wird die Syntax dieser AFS-Befehle erläutert, die Regeln, die bei der Ausführung der Befehle befolgt werden müssen, und die Art und Weise, wie auf die zugehörigen Hilfetexte zugegriffen wird.

AFS-Befehlssyntax

Die meisten AFS-Befehle verwenden die folgende Syntax:

Befehlsgruppe Operationscode -Schalter <*Wert*>[+] **-Markierung**

Mit *Befehlsgruppe* werden der allgemeine Befehlstyp und der Server-Prozeß, mit dem der Befehl ausgeführt wird, angegeben. Regelmäßige AFS-Benutzer haben Zugriff auf zwei Hauptbefehlsgruppen und eine Befehlsgruppe, die sonstige Befehle enthält:

- Die Befehlsgruppe **fs** wird verwendet, um Datei-Server-Befehle auszuführen, die mit dem File Server-Prozeß interagieren.
- Die Befehlsgruppe **pts** wird verwendet, um Befehle bezüglich Zugriffsschutz auszuführen.
- Die sonstigen Befehle sind keiner Befehlsgruppe zugeordnet.

Mit *Operationscode* wird die Aktion angegeben, die der Befehl ausführt. Die sonstigen Befehle verfügen nur über Operationscodes.

Ein Befehl kann über mehrere *Optionen* verfügen, die *Argumente* oder *Markierungen* sein können:

- Argumente werden verwendet, um zusätzliche Informationen zur Verwendung durch den Befehl zur Verfügung zu stellen. Sie bestehen aus einer Kombination aus einem *Schalter* und einer *Instanz*. Mit dem Schalter wird der Argumenttyp definiert. Vor dem Schalter steht immer ein Silbentrennungsstrich. Argumente können mehrere Instanzen annehmen, wenn nach der Instanz ein Pluszeichen (+) angegeben wird. Eine Instanz steht für eine variable Information, die von dem Befehl verwendet wird. Die Angabe von Argumenten kann optional oder erforderlich sein.
- Markierungen werden verwendet, um einen Befehl so zu steuern, daß er in einer bestimmten Art und Weise ausgeführt wird (um zum Beispiel einen

© Copyright IBM Corp. 1989, 2000

bestimmten Ausgabetyp zu generieren). Markierungen wird immer ein Silbentrennungsstrich vorangestellt, und sie sind immer optional.

Beispiel für die Befehlssyntax

In diesem AFS-Befehl gilt folgendes:

```
% fs setacl -dir $HOME -acl pat all terry none -negative
```

- **fs** ist die Befehlsgruppe.
- **setacl** ist der *Operationscode*, der den File Server-Prozeß dahingehend steuert, daß eine Zugriffssteuerungsliste definiert wird.
- **-dir $HOME** und **-acl pat all terry none** sind *Argumente*.
  - **-dir** und **-acl** sind Schalter. **-dir** gibt den Namen des Verzeichnisses an, für das die ACL definiert werden soll, und **-acl** definiert die Einträge, die darin festgelegt werden sollen.
  - **$HOME** und **pat all terry none** sind *Instanzen* der Argumente. **$HOME** definiert ein bestimmtes Verzeichnis für das Verzeichnisargument. Das Argument **-acl** verfügt über zwei Instanzen, die zwei ACL-Einträge angeben: **pat all** und **terry none**.
- **-negative** ist eine Markierung. Sie steuert den Befehl dahingehend, daß die Zugriffslisteneinträge in die Liste mit den negativen Berechtigungen, und nicht in die Liste mit den normalen Berechtigungen gestellt werden.

Regeln zur Verwendung von AFS-Befehlen

In diesem Abschnitt werden die Regeln beschrieben, die bei der Verwendung von AFS-Befehlen befolgt werden müssen.

Leerzeichen und Zeilen

Trennen Sie die einzelnen Befehlselemente (Befehlsgruppe, Operationscode, Schalter, Instanzen und Markierungen) durch Leerzeichen voneinander. Mehrere Instanzen eines Arguments werden auch durch ein Leerzeichen voneinander getrennt.

Geben Sie alle AFS-Befehle in einer Zeile ein, gefolgt von einer Zeilenschaltung. Einige Befehle in diesem Dokument werden in mehr als einer Zeile angezeigt. Dies geschieht jedoch nur aus Gründen der besseren Lesbarkeit.

Abkürzungen und Aliasnamen für Operationscodes

Den Operationscode können Sie in einer der drei folgenden Arten eingeben:

- Sie können den Operationscode in der Langform angeben.
- Sie können den Operationscode mit der kürzesten Abkürzung angeben, die ihn von den anderen Operationscodes in dieser Befehlsgruppe unterscheidet.
- Sie können den Aliasnamen für den Operationscode verwenden, wenn ein Aliasname vorhanden ist.

Zum Beispiel kann der Befehl **fs listacl** wie folgt abgesetzt werden:

- **fs listacl** (Befehl in der Langform)
- **fs lista** (Abkürzung)
- **fs la** (Aliasname)

Informationen zu der Befehlssyntax in der Lang- und Kurzform sowie zu Aliasnamen für alle in dieser Veröffentlichung diskutierten Befehle enthält die Veröffentlichung *AFS Administration Reference*.

Weglassen von Argumentschaltern

Sie können den Argumentschalter weglassen, wenn in dem Befehl nur ein Argument vorkommt oder wenn die folgenden Bedingungen erfüllt sind:

- Alle für den Befehl erforderlichen Argumente werden in der Reihenfolge aufgeführt, die durch die Syntaxanweisung vorgeschrieben ist.
- Es werden für keine Argumente Schalter verwendet, auch wenn sie in der korrekten Reihenfolge aufgeführt sind.
- Es gibt nur einen Wert für jedes Argument. Zu dieser Bedingung gibt es eine wichtige Ausnahme: Das letzte erforderliche Argument akzeptiert mehrere Werte. In diesem Fall ist es akzeptabel, mehrere Werte anzugeben, ohne den Schalter anzugeben.

Zum Beispiel sind die folgenden beiden Befehle äquivalent:

```
% fs setacl -dir /afs/abc.com/usr/terry/private -acl pat rl
% fs setacl /afs/abc.com/usr/terry/private pat rl
```

Der folgende Befehl ist jedoch keine akzeptable Kurzform, da die Argumente nicht in der vorgeschriebenen Reihenfolge aufgeführt sind:

```
% fs setacl -acl pat rl /afs/abc.com/usr/terry/private
```

Abkürzungen für Schalter und Markierungen

Wenn Sie einen Schalter verwenden müssen oder wenn Sie entscheiden, eine Markierung zu verwenden, können Sie in vielen Fällen eine Abkürzung für den Namen dieses Schalters oder dieser Markierung verwenden. Dies gilt unter der Voraussetzung, daß sich die Abkürzung von den anderen Markierungen und Schaltern des Befehls unterscheidet.

Wenn Sie zum Beispiel den Befehl **fs setacl** absetzen, können Sie alle Schalter und Markierungen des Befehls mit deren Anfangsbuchstaben abkürzen, da diese alle mit einem anderen Buchstaben beginnen. Wenn Sie jedoch den Befehl **knfs** absetzen, beginnen das Argument **-host** und die Markierung **-help** beide mit dem Buchstaben **h**. Die kürzesten eindeutigen Abkürzungen sind daher **-ho** bzw. **-he**.

Abkürzungen für Verzeichnisreferenzen

Die meisten AFS-Befehlsargumente, die Verzeichnis- und Pfadnamensinstanzen erfordern, akzeptieren eine oder mehrere der folgenden Kurzformen:

- Ein einzelner Punkt (**.**) gibt das aktuelle Arbeitsverzeichnis an.
- Zwei Punkte (**..**) geben das Elternverzeichnis des aktuellen Arbeitsverzeichnisses an.
- Die Umgebungsvariable $HOME gibt das Ausgangsverzeichnis des Benutzers an, der den Befehl absetzt.

Wenn zum Beispiel Benutzer **terry** seinem Manager **pat** die Berechtigungen **r** (**read**) und **l** (**lookup**) für sein Ausgangsverzeichnis erteilen möchte, kann **terry** folgenden Befehl absetzen:

```
% fs setacl -dir $HOME -acl pat rl
```

Wenn das aktuelle Arbeitsverzeichnis das Ausgangsverzeichnis des Benutzers **terry** ist, kann er den folgenden Befehl absetzen:

```
% fs setacl -dir  .  -acl pat rl
```

Beide der vorherigen Beispiele sind akzeptable Kurzformen für den folgenden Befehl:

```
% fs setacl -dir /afs/abc.com/usr/terry -acl pat rl
```

Häufig verwendete fs- und pts-Befehle

Dieser Abschnitt enthält weitere Informationen zu den häufig verwendeten AFS-Befehlen der Befehlsgruppen **fs** und **pts**. Detaillierte Informationen dazu enthält die Veröffentlichung *AFS Administration Reference*.

Informationen zu den fs-Befehlen

Mit einigen **fs**-Befehlen wird die UNIX-Dateisystemsemantik erweitert, indem dateibezogene Funktionen aufgerufen werden, die UNIX nicht zur Verfügung stellt (zum Beispiel das Definieren von Zugriffssteuerungslisten). Mit anderen **fs**-Befehlen wird die Leistung des Cache Managers gesteuert, der auf der lokalen Client-Maschine ausgeführt wird.

Alle **fs**-Befehle akzeptieren die optionale Markierung **-help**. Die Markierung hat dieselbe Funktion wie der Befehl **fs help**: Mit ihr wird die Online-Hilfenachricht für einen Befehl auf den Bildschirm emittiert. Geben Sie gleichzeitig mit dieser Markierung keine anderen Optionen an. Die Markierung setzt andere Optionen nämlich außer Kraft. Der einzige Effekt bei der Ausführung des Befehls ist das Anzeigen der Hilfenachricht.

Welche Berechtigung zur Ausführung von **fs**-Befehlen erforderlich ist, ist verschieden. Zu den Berechtigungen, die für die in dieser Veröffentlichung beschriebenen **fs**-Befehle erforderlich sind, gehören folgende:

- Bestimmte Berechtigungen für die Zugriffssteuerungsliste eines Verzeichnisses. Zum Beispiel sind für das Erstellen und das Entfernen von Mount-Punkten die Berechtigungen **a** (**administer**), **i** (**insert**) und **d** (**delete**) für das Verzeichnis erforderlich, in dem sich der Mount-Punkt befindet.
- Zugehörigkeit zu der Gruppe **system:administrators** (siehe „Verwenden von Systemverwaltungsgruppen in ACLs" auf Seite 38).
- Keine Berechtigung. Mit vielen **fs**-Befehlen werden einfach nur Informationen aufgelistet. Für diese Befehle sind daher keine besonderen Berechtigungen erforderlich.

Informationen zu den pts-Befehlen

Die Befehlsgruppe **pts** ist die Schnittstelle, über die Sie Zugriffsschutzgruppen erstellen und diesen Mitglieder hinzufügen können. Systemadministratoren, die zu einer bestimmten Systemgruppe mit dem Namen **system:administrators** gehören, können jede Gruppe verändern und auch die Benutzer- und Maschineneinträge erstellen, die zu Gruppen gehören können. Benutzer, die nicht zu der Gruppe **system:administrators** gehören, können stets die Informationen auflisten, die den Gruppeneinträgen zugeordnet sind, deren Eigner sie sind, sowie die Benutzereinträge, deren Eigner sie sind. Abhängig von der Definition der Markierungen für den Zugriffscode eines Eintrags, können regelmäßige Benutzer manchmal auf bestimmte Weise auf Gruppeneinträge zugreifen und diese bearbeiten.

Alle **pts**-Befehle akzeptieren optionale Argumente und Markierungen. Sie sind in den Befehlsbeschreibungen in der Veröffentlichung *AFS Administration Reference* aufgelistet und werden dort im Detail beschrieben:

[-cell <*Zellenname*>**]**

Mit diesem Argument wird angegeben, daß der Befehl in der angegebenen Zelle ausgeführt wird. Der Benutzer, der den Befehl absetzt, kann für den Wert für *Zellenname* die kürzeste Form angeben, die den Zellennamen von anderen Zellen unterscheidet, die in der Datei **/usr/vice/etc/CellServDB** auf der Client-Maschine aufgelistet sind, auf der der Befehl abgesetzt wird. Standardmäßig werden die Befehle in der lokalen Zelle ausgeführt, die definiert ist durch

- erstens - den Wert der Umgebungsvariable AFSCELL. (Diese Variable ist normalerweise nicht durch einen Standardwert definiert. Wenn Sie über einen längeren Zeitraum hinweg in einer anderen, nicht lokalen Zelle arbeiten, können Sie für die Variable den Namen dieser Zelle festlegen.)
- zweitens - die Datei **/usr/vice/etc/ThisCell** auf der Client-Maschine, auf der der Befehl abgesetzt wird.

[-force]

Mit dieser Markierung wird der Befehls-Interpreter **pts** dahingehend gesteuert, daß er die Ausführung des Befehls fortführt, wenn möglich, selbst dann, wenn Probleme bei der Ausführung des Befehls auftreten. Wenn der Befehls-Interpreter auf ein Problem trifft, führt er soviel der angeforderten Operation wie möglich durch, und hält die Ausführung nicht an. Der Befehls-Interpreter meldet alle Fehler, auf die er während der Ausführung des Befehls trifft. Diese Markierung ist besonders nützlich, wenn viele Instanzen für ein Argument angegeben werden. Wenn in einem solchen Fall eine der Instanzen ungültig ist, meldet der Befehl den Fehler und fährt mit der Ausführung der restlichen Argumente fort.

[-help]

Diese Markierung hat dieselbe Funktion wie der Befehl **pts help**: Mit ihr wird die Online-Hilfenachricht für einen Befehl auf den Bildschirm emittiert. Geben Sie gleichzeitig mit dieser Markierung keine anderen Optionen an. Die Markierung setzt andere Optionen nämlich außer Kraft. Der einzige Effekt bei der Ausführung des Befehls ist das Anzeigen der Hilfenachricht.

Anfordern von Hilfe in AFS

Die AFS-Online-Hilfefunktion besteht aus Basissyntaxnachrichten. Die AFS-Verteilung enthält auch Hilfe im HTML-Format, die Ihnen Ihr Systemadministrator zur Verfügung stellen kann.

Anzeigen von Befehlssyntax und Aliasnamen

Zum Anzeigen der Kurzbeschreibung eines Befehls, dessen Syntaxanweisung und ggf. Aliasnamen, verwenden Sie den Operationscode **help**. Um zum Beispiel den Online-Hilfeeintrag für den Befehl **fs listacl** anzuzeigen, geben Sie den folgenden Befehl ein:

```
% fs help listacl
fs listacl: list access control list
aliases: la
Usage: fs listacl  [-path <Verzeichnis-/Dateipfad>+]  [-id] [-if] [-help]
```

Wenn nur die Syntaxanweisung angezeigt werden soll, verwenden Sie die Markierung **-help**, die in den meisten AFS-Befehlen zur Verfügung steht. Um zum Beispiel die Syntaxanweisung für den Befehl **fs setacl** anzuzeigen, geben Sie den folgenden Befehl ein:

```
% fs setacl -help
Usage: fs setacl -dir <Verzeichnis>+ -acl <Zugriffslisteneinträge>+ [-clear] [-negativ
[-id] [-if] [-help]
```

Anzeigen von Beschreibungen des Operationscodes

Zum Anzeigen einer kurzen Beschreibung aller Operationscodes einer Befehlsgruppe geben Sie den Operationscode **help** ohne andere Argumente an. Zum Beispiel wird mit dem Befehl **fs help** eine Kurzbeschreibung jedes Operationscodes in der Befehlsgruppe **fs** angezeigt.

Um die Befehle in einer Befehlsgruppe aufzulisten, die einen bestimmten Objekttyp betreffen, geben Sie für den Operationscode **apropos** ein entsprechendes Schlüsselwortargument an. Wenn Sie zum Beispiel eine ACL definieren möchten, sich aber nicht daran erinnern können, welcher **fs**-Befehl verwendet wird, führen Sie den folgenden Befehl aus:

```
% fs apropos set
setacl: set access control list
setcachesize: set cache size
setcell: set cell status
setclientaddrs: set client network interface addresses
setquota: set volume quota
setserverprefs: set file server ranks
setvol: set volume status
sysname: get/set sysname (i.e. @sys) value
```

Die folgende Nachricht gibt an, daß keine Befehle vorhanden sind, deren Namen oder Beschreibungen das angegebene Schlüsselwort enthalten:

```
Sorry, no commands found
```

Anmerkung: Wenn das von Ihnen angegebene Schlüsselwort Leerzeichen enthält, setzen Sie es in Anführungszeichen (″ ″).

Anhang C. Glossar

a (administer)-Berechtigung
Die ACL-Berechtigung, die es ihrem Besitzer erlaubt, die Einträge in der ACL zu ändern.

Zugriffscodemarkierung a
Die vierte Zugriffscodemarkierung einer Gruppe, die es Ihrem Besitzer erlaubt, Mitglieder zu ihr hinzuzufügen.

Zugriffssteuerungsliste (ACL = Access Control List)
Einem AFS-Verzeichnis zugeordnete Liste, die angibt, welche Aktionen ein Benutzer oder eine Gruppe bezüglich des Verzeichnisses und der Dateien in ihm ausführen kann. Es gibt sieben Zugriffsberechtigungen: **a** (**adminsiter**), **d** (**delete**), **i** (**insert**), **k** (**lock**), **l** (**lookup**), **r** (**read**) und **w** (**write**).

ACL-Eintrag
Ein Eintrag in einer ACL, der einen Benutzer oder eine Gruppe mit speziellen Zugriffsberechtigungen verbindet.

Alias Ein alternativer Name für einen AFS-Befehl.

ACL-Kurzschrift all
Eine verkürzte Schreibweise, die mit dem Befehl **fs setacl** verwendet wird, um alle sieben Berechtigungen zu repräsentieren.

Anonym
Die Identität, die einem Benutzer zugewiesen wird, der für die lokale Zelle kein gültiges Token besitzt.

Argument
Der Bestandteil eines Befehls, der eine Entity bezeichnet, die durch den Befehl beeinflußt werden soll. Argumente bestehen aus zwei Teilen: Einem *Schalter* und einer oder mehreren *Instanzen*. Einige AFS-Befehle benötigen ein oder mehrere Argumente.

Authentifizieren
Angeben des korrekten Kennworts, um als gültiger AFS-Benutzer erkannt zu werden. Authentifizieren Sie sich durch Anmelden bei einer Maschine, die ein für AFS modifiziertes Anmeldedienst-programm verwendet, oder durch Eingeben des Befehls **klog**. Nur authentifizierte Benutzer können die meisten AFS-Aktionen ausführen.

Byte, Kilobyte
Eine Maßeinheit, die zum Messen der Speicherplatzbelegung auf einem Volume oder einer Partition verwendet wird. Ein Kilobyte entspricht 1024 Bytes.

© Copyright IBM Corp. 1989, 2000

Cache Manager
Ein Satz von Modifikationen des Betriebssystems auf einer Client-Maschine, der es Benutzern ermöglicht, auf der Maschine auf in AFS gespeicherte Dateien zuzugreifen. Der Cache Manager fordert Dateien vom File Server an und speichert (*zwischenspeichert*) eine Kopie jeder Datei auf der lokalen Platte der Client-Maschine. Anwendungsprogramme verwenden dann die im Cache befindliche Kopie, womit wiederholte Netzanforderungen an die Datei-Server-Maschinen vermieden werden.

Im Cache befindliche Datei
Eine Kopie einer Datei, die der Cache Manager auf der lokalen Platte der Workstation speichert.

Rückruf
Eine Zusage des File Servers, den Cache Manager zu kontaktieren, wenn die zentral gespeicherte Kopie der Datei verändert wird, während der Cache Manager eine Kopie davon im Cache hat. Wenn die Datei verändert wird, *unterbricht* der File Server den Rückruf. Wenn ein Anwendungsprogramm das nächste Mal Daten von der Datei anfordert, nimmt der Cache Manager den unterbrochenen Rückruf an und erhält vom File Server eine aktualisierte Kopie der Datei. Rückrufe gewährleisten, daß der Benutzer mit der jeweils aktuellen Kopie einer Datei arbeiten kann.

Zelle Ein unabhängig verwalteter Standort mit aktivem AFS, der aus einer Ansammlung von Datei-Server-Maschinen und Client-Maschinen besteht, die als zur Zelle zugehörig definiert wurden. Eine Maschine kann zu einem beliebigen Zeitpunkt immer nur zu einer Zelle gehören.

Client-Maschinen
Computer, die für Benutzer Berechnungen ausführt. Normalerweise arbeiten Benutzer auf einer Client-Maschine und greifen auf Daten zu, die sich auf einer Datei-Server-Maschine befinden.

Client/Server-Betrieb
Ein Verarbeitungssystem, in dem zwei Typen von Computern (Client-Maschinen und Server-Maschinen) verschiedene spezialisierte Funktionen ausführen.

Befehl Eine Zeichenfolge, die einem AFS-Server eine auszuführende Aktion angibt. Eine Beschreibung der AFS-Befehlssyntax finden Sie in „Anhang B. AFS-Befehlssyntax und Online-Hilfefunktion” auf Seite 81.

Befehlsgruppe
Eine Gruppe von AFS-Befehlen mit zusammengehörenden Funktionen. Der Name der Befehlsgruppe ist in vielen AFS-Befehlen das erste Wort.

Vollständiger Pfadname
Eine vollständige Spezifikation des Speicherorts einer Datei in AFS, die an der Wurzel des Dateibereichs (gemäß Konvention das Verzeichnis **/afs**) beginnt und alle Verzeichnisse angibt, die der Cache Manager passieren muß, um auf die Datei zuzugreifen. Die Namen der Verzeichnisse werden durch Schrägstriche getrennt.

d (delete)-Berechtigung
Die ACL-Berechtigung, die es ihrem Besitzer erlaubt, Elemente aus einem Verzeichnis zu entfernen.

Verzeichnis
Eine logische Struktur, die eine Ansammlung von Dateien und anderen Verzeichnissen enthält.

Verteiltes Dateisystem
Ein Dateisystem, das die Dateisysteme einzelner Maschinen miteinander verknüpft. Die Dateien sind auf verschiedenen Maschinen im Netzwerk gespeichert, auf sie kann aber von allen Maschinen aus zugegriffen werden.

Datei Eine Zusammenfassung von Informationen, die als Einheit gespeichert und abgerufen werden.

Datei-Server-Maschine
Ein Maschinentyp, der Dateien speichert und sie auf Anforderung zu Client-Maschinen überträgt.

Markierung
Teil eines Befehls, der bestimmt, wie der Befehl ausgeführt wird, oder die zu erzeugende Ausgabe festlegt.

Fremde Zelle
Eine Zelle, die nicht zur Client-Maschine gehört. Wenn die Client-Maschine entsprechend konfiguriert ist, können die Benutzer auf den AFS-Dateibereich in fremden Zellen genauso wie in der lokalen Zelle zugreifen, und Sie können sich in den fremden Zelle authentifizieren, in denen Sie AFS-Konten besitzen.

Gruppe
Eine definierte Liste von Benutzern in der ACL eines Verzeichnisses, mit deren Hilfe ein Satz von Berechtigungen für alle ihre Mitglieder gültig wird.

Gruppe, die einer Gruppe gehört
Eine Gruppe, die einer anderen Gruppe gehört. Alle Mitglieder der Eignergruppe können die untergeordnete Gruppe verwalten; die Mitglieder der untergeordneten Gruppe haben auf sich selbst bezogen keine Verwaltungsberechtigungen.

Hierarchische Dateistruktur
Eine Methode des Speicherns von Daten in Verzeichnissen, die als Baumstruktur organisiert sind.

Ausgangsverzeichnis
Ein Verzeichnis, das einem Benutzer gehört und für die Speicherung der persönlichen Dateien des Benutzers vorgesehen ist.

i (insert)-Berechtigung
Die ACL-Berechtigung, die es ihrem Besitzer erlaubt, Dateien oder Unterverzeichnisse zu einem Verzeichnis hinzuzufügen.

Instanz
Der Teil einer Befehlsfolge, der die betroffene Entity definiert.

k (lock)-Berechtigung
Siehe Eintrag k (lock)-Berechtigung. Die ACL-Berechtigung, die es Programmen erlaubt, eine Datei mit Informationssperren zu versehen.

Kilobyte
Eine Maßeinheit, die zum Messen der Speicherplatzbelegung auf einem Volume oder einer Partition verwendet wird. Ein Kilobyte entspricht 1024 Bytes. Der Begriff *Kilobyte-Block* wenn manchmal für Verweise auf Plattenspeicherplatz verwendet.

l (lookup)-Berechtigung
Die ACL-Berechtigung, die es ihrem Besitzer erlaubt, den Inhalt eines Verzeichnisses und seine ACL aufzulisten.

Lokale Zelle
Die Zelle, zu der das Benutzerkonto und die Client-Maschine gehören.

lock-Berechtigung
Siehe Eintrag **k (lock)-Berechtigung**.

Anmelden
Das Herstellen einer Verbindung zum Dateisystem einer Client-Maschine als einem speziellen Benutzer.

Abmelden
Das Beenden einer Verbindung zum lokalen Dateisystem.

Zugriffscodemarkierung m
Die dritte Zugriffscodemarkierung einer Gruppe, die es Ihrem Besitzer erlaubt, die Mitglieder einer Gruppe oder die Gruppen, zu denen ein Benutzer gehört, aufzulisten.

Modusbits
Ein Satz von Berechtigungen, die das UNIX-Dateisystem mit einer Datei oder einem Verzeichnis verknüpft, um den Zugriff darauf zu steuern. Sie erscheinen im ersten Feld der Ausgabe des Befehls **ls -l**.

Mount-Punkt
Eine spezieller Verzeichnistyp, der einen Speicherort im AFS-Dateibereich mit einem Volume verknüpft. Er agiert als ein Standard-UNIX-Verzeichnis, in das Benutzer wechseln und dessen Inhalt sie mit den UNIX-Befehlen **cd** und **ls** anzeigen können.

Gegenseitige Authentifizierung
Eine Prozedur, mit deren Hilfe zwei Teilnehmer einander ihre Identität nachweisen. AFS-Server- und Client-Prozesse authentifizieren sich üblicherweise gegenseitig, wenn sie eine Verbindung herstellen.

NFS/AFS Translator
Ein Programm, das es den Benutzern von NFS-Client-Maschinen erlaubt, auf Dateien im AFS-Dateibereich zuzugreifen.

ACL-Kurzschrift none
Eine verkürzte Schreibweise, die mit dem Befehl **fs setacl** verwendet wird, um einen Eintrag aus einer ACL zu löschen.

Zugriffscodemarkierung o
Die zweite Zugriffscodemarkierung einer Gruppe, die es Ihrem Besitzer erlaubt, die Gruppen, die einem Benutzer oder einer Gruppe gehören, aufzulisten.

Operationscode
Das zweite Wort in einem AFS-Befehl, der zu einer bestimmten Gruppe gehört. Es gibt die Funktion des Befehls an.

Eigner einer Gruppe
Die Person oder Gruppe, die eine Gruppe verwalten kann.

Elternverzeichnis
Das Verzeichnis, in dem sich ein Verzeichnis oder Dateien befinden.

Partition
Ein logischer Plattenbereich in einem Computer.

Kennwort
Eine eindeutige, benutzerdefinierte Zeichenfolge, die der Systemidentität des Benutzers Gültigkeit verleiht. Der Benutzer muß das Kennwort korrekt eingeben, um authentifiziert zu werden.

Berechtigung
Ein bestimmter Zugriffstyp, der einer ACL verliehen wurde. Jeder, der die Berechtigung besitzt, kann die Aktion ausführen.

Quote Die Begrenzung der Größe eines Volumes, die durch den Systemadministrator zugewiesen und in Kilobyte-Blöcken gemessen wird.

r (read)-Berechtigung
Die ACL-Berechtigung, die es ihrem Besitzer erlaubt, den Inhalt einer Datei zu prüfen.

Zugriffscodemarkierung r
Die fünfte Zugriffscodemarkierung einer Gruppe, die es Ihrem Besitzer erlaubt, Mitglieder aus ihr zu entfernen.

ACL-Kurzschrift read
Eine verkürzte Schreibweise, die mit dem Befehl **fs setacl** verwendet wird, um die Berechtigungen **r** und **l** zu repräsentieren.

Relativer Pfadname
Ein Pfadname, der nicht beim Stammverzeichnis von AFS oder des lokalen Dateibereichs beginnt, und damit den Speicherort einer Datei oder eines Verzeichnisses in Relation zum aktuellen Arbeitsverzeichnis darstellt.

Ferne Befehle
Die Befehle, die dazu verwendet werden, Programme auf einer fernen Maschine auszuführen, ohne eine Verbindung mit ihr herstellen zu müssen.

Zugriffscodemarkierung s
Die erste Zugriffscodemarkierung einer Gruppe, die es Ihrem Besitzer erlaubt, Basisinformationen über sie aufzulisten.

Gruppe, die sich selbst gehört
Eine Gruppe, deren Eigner sie selbst ist, und die es damit allen ihren Mitgliedern erlaubt, sie zu verwalten.

Server Ein Programm oder eine Maschine, das oder die seinen oder ihren Clients einen speziellen Service zur Verfügung stellt, wie das Speichern und Übertragen von Dateien oder das Ausführen der Authentifizierung.

Unterverzeichnis
Ein Verzeichnis, das sich innerhalb der Systemhierarchie in einem anderen Verzeichnis befindet.

Schalter
Der Teil einer Befehlsfolge, der den Typ eines Argumentes definiert. Ihm wird ein Silbentrennungsstrich vorangestellt.

Syntaxanweisung
Eine Spezifikation der für einen Befehl verfügbaren Optionen und ihrer Reihenfolge.

Systemadministrator
Ein Benutzer, der zum Verwalten einer AFS-Zelle berechtigt ist.

Systemverwaltungsgruppen
Gruppen, die AFS automatisch definiert, um Benutzer zu repräsentie-

ren, die bestimmte Kenndaten gemeinsam benutzen. Siehe auch die drei Einträge: Gruppe system:administrators, Gruppe system:anyuser und Gruppe system:authuser.

Gruppe system:administrators
Eine Systemverwaltungsgruppe mit Benutzern, die zum Verwalten von AFS berechtigt sind.

Gruppe system:anyuser
Eine Systemverwaltungsgruppe. die jeden enthält, der auf den AFS-Dateibereich zugreifen kann. Sie enthält nicht authentifizierte Benutzer, denen die Identität **anonym** zugewiesen wird.

Gruppe system:authuser
Eine Systemverwaltungsgruppe mit allen Benutzern, die aktuell gültige AFS-Token für die lokale Zelle besitzen.

Token Eine Zusammenfassung von Daten, die der AFS-Server als Beweis dafür akzeptiert, daß der Besitzer seine Identität gegenüber dem AFS-Authentifizierungsservice erfolgreich nachgewiesen hat. AFS weist Benutzern, die kein Token besitzen, die Identität **anonym** zu.

UNIX-Modusbits
Siehe Eintrag **Modusbits**.

Benutzername
Eine beim Anmelden eingegebene Zeichenfolge, die eine Person gegenüber der lokalen Zelle eindeutig identifiziert.

Volume
Eine durch AFS für Verwaltungszwecke verwendete Struktur zum Gruppieren von Dateien und Verzeichnissen in einer einzigen Einheit. Der Inhalt eines Volumes befindet sich auf einer einzigen Plattenpartition und kann nur über einen Mount-Punkt im AFS-Dateibereich erreicht werden.

w (write)-Berechtigung
Die ACL-Berechtigung, die es ihrem Besitzer erlaubt, den Inhalt einer Datei zu verändern.

ACL-Kurzschrift write
Eine verkürzte Schreibweise, die mit dem Befehl **fs setacl** verwendet wird, um alle Berechtigungen mit Ausnahme der Berechtigung **a** zu repräsentieren.

Index

A

Abbrechen einer AFS-Sitzung 19
Abmelden 19
ACL
  alle Einträge ersetzen 46
  anzeigen 40
  beschrieben 7, 33
  definieren 42
  definierte Berechtigungen 34
  eigener Eintrag versehentlich entfernt 72
  Eintrag für negative Berechtigung erstellen 45
  Eintrag für normale Berechtigung 43
  Entfernen veralteter Einträge 61
  fremde Benutzer in ACL 38
  im Vergleich zu UNIX-Modusbits 9
  Inhalt löschen 46
  Kurzform für Mengen an Berechtigungen 36
  negative Berechtigungen 37
  normale Berechtigungen 37
  normale und negative Berechtigungen 37
  von einem Verzeichnis in ein anderes kopieren 48
  zusätzliche Berechtigungen 36
ACL-Berechtigung a 35
ACL-Berechtigung administer 35
ACL-Berechtigung d 35
ACL-Berechtigung delete 35
ACL-Berechtigung i 35
ACL-Berechtigung insert 35
ACL-Berechtigung k 36
ACL-Berechtigung l 35
ACL-Berechtigung lock 36
ACL-Berechtigung lookup 35
ACL-Berechtigung r 36
ACL-Berechtigung read 36
ACL-Berechtigung w 36
ACL-Berechtigung write 36
AFS
  Dateibereich als Erweiterung des lokalen Dateibereichs 2
  Informationen zur gemeinsame Benutzung 1
  Sicherheit 6
AFS *(Forts.)*
  transparenter Zugriff 1
  UIDs und GIDs 57
  Zugreifen auf Dateibereich 21
  Zugriff von der NFS-Client-Maschine 75
afs: failed to store file (Fehlernachricht) 73
all, Kurzform für ACL-Berechtigungen 36
Alle ACL-Einträge löschen 46

Ä

Ändern
  ACLs 42
  AFS-Kennwort 24
  Eigner der Gruppe 63
  Gruppenname 63
  UNIX-Kennwort 24
Anmeldedienstprogramm 11, 13
Anmelden 13
Anzeigen
  Ablaufdatum des Kennworts 23
  ACL-Einträge 40
  Datei-/Verzeichnisposition 28
  Eigner der Gruppe 57
  Ersteller der Gruppe 57
  Gruppen, die einer Gruppe gehören 56
  Gruppenerstellungsquote 57
  Gruppeninformationen 55
  Prozentsatz der verwendeten Quote eines Volumes 26
  Prozentsatz des verwendeten Speicherbereichs einer Plattenpartition 26
  Quote eines Volumes mit weiteren Informationen 26, 27
  Token 17
  verfügbarer Speicherplatz auf der Plattenpartition und Gesamtgröße 27
  Verzeichnis-/Dateiposition 28
  Wiederverwendungsmaßnahme des Kennworts 23
Argument setpag zum Befehl klog 15
Argumente für AFS-Befehle 81
Authentifizierung
  als ein anderer Benutzer 16
Authentifizierung *(Forts.)*
  Begrenzung von nacheinander fehlgeschlagenen Versuchen 18
  bei DCE für DFS-Zugriff 16
  definiert 6
  für AFS auf NFS-Client-Maschinen 76
  gegenseitig 6
  in einer fremden Zelle 15
  Token als Nachweis 14

B

Beenden einer AFS-Sitzung 19
Befehl chgrp 10
Befehl chmod 10, 51
Befehl chown 10
Befehl dlog 16
Befehl dpass 16
Befehl ftp 10
Befehl groups 10
Befehl inetd 11
Befehl klog 16
Befehl knfs 77
Befehl kpasswd 24
Befehl ln 11
Befehl rcp 10
Befehl rsh 10
Befehl unlog 20
Befehle
  AFS-Befehle, von NFS-Client-Maschine aus absetzen 75
  Befehlsgruppen in AFS 81
  chgrp 10
  chmod 10, 51
  chown 10
  dlog 16
  dpass 16
  fs checkservers 29
  fs cleanacl 62
  fs copyacl 49
  fs examine 27
  fs getserverprefs 31
  fs listacl 40
  fs listcells 30
  fs listquota 26
  fs quota 26
  fs setacl 43, 45
  fs whereis 28
  ftp 10
  groups 10

© Copyright IBM Corp. 1989, 2000

Befehle *(Forts.)*
inetd 11
kas examine 19, 23
klog 16
knfs 77
kpasswd 24
ln 11
login 13
passwd 24
pts adduser 60
pts chown 63
pts creategroup 59
pts delete 62
pts examine 57
pts listowned 56
pts membership 56
pts removeuser 61
pts rename 64
pts setfields 66
rcp 10
rsh 10
Syntax für AFS 81
tokens 17
unlog 20
Befehle kas
examine 19, 23
Befehlsgruppen bei AFS-Befehlen 81
Begrenzung von Authentifizierungsversuchen 19
Beispiele
ACL für ein einzelnes Verzeichnis anzeigen 41
ACL von einem Verzeichnis in ein anderes kopieren 49
ACLs für mehrere Verzeichnisse anzeigen 42
Ändern des Eigners der Gruppe 64
Ändern des Gruppennamens 65
Anzeigen der Gruppen, die einem Benutzer gehören 57
Anzeigen der Gruppen, die einer Gruppe gehören 57
Anzeigen der Mitglieder einer Gruppe 56
Anzeigen der Quote eines Volumes und anderer Informationen 27
Anzeigen des verwendeten Prozentsatzes der Quote eines Volumes 26
Anzeigen von Gruppeninformationen über einen Benutzer 58
Beispiele *(Forts.)*
Anzeigen von Informationen über Gruppen 58
Authentifizieren 17
Authentifizieren als ein anderer Benutzer 18
Authentifizieren in einer fremden Zelle 18
Benutzer einer ACL hinzufügen 44
chmod verwenden 51
Deauthentifizieren von ausgewählten Zellen 20
eine ACL ersetzen 47
Einstellen der Zugriffscodemarkierungen einer Gruppe 67
Eintrag im Abschnitt mit den negativen Berechtigungen in der ACL erstellen 45
Entfernen gelöschter Gruppen aus ACLs 62
Entfernen von Gruppenmitgliedern 62
Erstellen einer Gruppe 60
Erstellen einer Gruppe, die sich selbst gehört 64
Hinzufügen von Mitglieder zu einer Gruppe 61
Informationen zum Volume anzeigen 27
Interaktion zwischen Volume und Mount-Punkt 3
Löschen einer Gruppe 62
mehrere Dateien suchen 28
Status von Datei-Servern überprüfen 30
Benutzer
Anzeigen der Anzahl von Gruppenzugehörigkeiten 57
Anzeigen von Gruppeninformationen 55
Auflisten der eigenen Gruppen 56
Entfernen aus Gruppen 61
Hinzufügen als Gruppenmitglieder 60
Sperrzeit für Konto 19
Berechtigungen in ACL
Anzeigen 40
definieren 42
definiert 34
Kurzform für 36
normale und negative 37
Berechtigungen in einer ACL definieren 42

C

Cache Manager
beschrieben 4
Datei-Server-Vorgaben anzeigen 31
Token, Verwendung von 14
Client-Maschine 1, 4
Client/Server-Betrieb 1
connection timed out (Fehlernachricht) 73

D

Datei-Server-Maschinen
Status überprüfen 29
Dateien
Aktualisieren 5
Fehler beim Zugriff, beim Kopieren oder Speichern 69
gemeinsame Benutzung 5, 8
in den Cache stellen 4
Standort anzeigen 28
Verweigern des Zugriffs 5
Zugreifen auf AFS 21
Zugriff erteilen 43
Zugriff verweigern 45
Dateien in den Cache stellen 4
Dateien kopieren
Fehler 69
Dateien sichern
auf Datei-Server-Maschinen, auf die nicht zugegriffen werden kann 29
Dateien speichern
Fehler 69
Deauthentifizieren 19
definierte Server-Maschinen 1

E

Entfernen
alle ACL-Einträge 46
Benutzer aus Gruppen 61
veraltete ACL-Einträge 61
Ersetzen
alle Einträge in der ACL 46
Erstellen
ACL als Kopie einer anderen ACL 48
ACL-Eintrag im Abschnitt mit den negativen Berechtigungen 45
ACL-Eintrag im Abschnitt mit normalen Berechtigungen 43
Gruppen 58
Erteilen von Zugriff auf AFS-Dateibereich 43

F

failed to store file (Fehlernachricht) 73
Fehlerbehebung
  Fehler bei Zugriff auf Datei, bei Kopieren oder Speichern der Datei 69
  Fehlernachrichten 73
  Versehentliches Entfernen aus ACL 72
Fehlernachrichten, Fehlerbehebung 73
ferne Befehle 10
Format von AFS-Pfadnamen 21
fremde Zellen
  definiert 3
Fremde Zellen
  Zugreifen 22
  Zugriff aktivieren 30
fs-Befehle
  checkservers 29
  cleanacl 62
  copyacl 49
  Einführung 84
  erforderliche Berechtigungen 84
  examine 27
  getserverprefs 31
  Hilfe anfordern 84
  listacl 40
  listcells 30
  listquota 26
  Markierung help 84
  quota 26
  setacl 43
    ACL vollständig ersetzen 47
    mit Markierung -negative 45
  whereis 28

G

Gegenseitige Authentifizierung 6
Gemeinsame Verwendung von Gruppen 54
GID, AFS 57
Gruppe, die sich selbst gehört 54
Gruppe system:anyuser
  Steuern des Zugriffs durch fremde Benutzer 22
Gruppen
  Ändern des Eigners 63
  Ändern des Namens 63
  Anzeigen von Informationen 55
  Auflisten der eigenen Gruppen 56
  Eigner, Anzeigen 57
  Eigner als Administrator 58
Gruppen *(Forts.)*
  Entfernen von Mitgliedern 61
  erstellen 58
  Ersteller, Anzeigen 57
  Erstellungsquote 55
  gemeinsame Verwendung 54
  Gruppen, die einer Gruppe gehören 54
  Gruppen, die sich selbst gehören 54
  Gruppenverwendung 54
  Hinzufügen von Mitgliedern 58, 60
  löschen 61
  Maschinen als Mitglieder 53
  Namenskonventionen 54
  private Verwendung 53
  Regeln für das Zuweisen des Eigentumsrechtes 59
  Zugriffscodemarkierungen 65
Gruppenerstellungsquote
  anzeigen 57
  definiert 55
Gruppenverwendung von Gruppen 54

H

Hilfe
  Beispiele 86
  Online-Hilfefunktion für AFS-Befehle 86
  Operationscode in AFS-Befehlsgruppen 86
Hinzufügen
  ACL-Eintrag, zum Abschnitt mit den negativen Berechtigungen 45
  ACL-Eintrag für Abschnitt mit normalen Berechtigungen 43
  Benutzer zu Gruppen 58

I

Instanzen bei AFS-Befehlen 81

K

Kennwort 6
  Ablaufdatum, Anzeigen 23
  Ändern von AFS 24
  Ändern von UNIX 24
  Wiederverwendungsmaßnahme, Anzeigen 23
Kommunikation
  zwischen Clients und Servern 1
  zwischen Zellen und Standorten 3
Kopieren
  ACL von einem Verzeichnis in ein anderes 48
Kurzform für ACL-Berechtigungen 36

L

Lebensdauer von Token 16
Lokale Kennwortdatei (/etc/passwd) 9
lokale Maschine 2
lokale Zelle, definiert 3
Löschen von Gruppen 61
lost contact with fileserver (Fehlernachricht) 73

M

Markierungen bei AFS-Befehlen 82
Maschinen
  als Mitglieder von Gruppen 53
  Client 1
  Server 1
Modusbits (UNIX)
  Interpretation in AFS 50
Mount-Punkte, definiert 3

N

Negative ACL-Berechtigungen
  definieren 37
  definiert 37
NFS
  AFS-Befehle von NFS-Client-Maschine aus absetzen 75
  Zugriff auf AFS vom Client 75
NFS/AFS Translator 75
none, Kurzform für ACL-Berechtigungen 36
Normale ACL-Berechtigungen
  definieren 37
  definiert 37

O

Online-Hilfefunktion 86
Operationscode apropos 86
Operationscodes in AFS-Befehlen
  abkürzen 82
  definiert 81

P

PAG 15
passwd
  Befehl 24
  Datei 9
Pfadnamen 21

Plattenpartition
Anzeigen des Prozentsatzes des verwendeten Speicherbereichs 26
Benutzung in AFS 3
Konsequenzen bei voller Quote 25
verfügbaren Speicherplatz und Gesamtgröße anzeigen 27
Private Verwendung von Gruppen 53
Prozeßauthentifizierungsgruppe (PAG) 15
pts-Befehle
adduser 60
chown 63
creategroup 59
delete 62
erforderliche Berechtigung 85
examine 57
Hilfe anfordern 86
listowned 56
Markierung force 86
Markierung help 86
removeuser 61
rename 64
setfields 66
Zellenargument 85
Zugehörigkeit 56

Q

Quote eines Volumes 25
Anzeigen mit weiteren Informationen 26, 27
verwendeten Prozentsatz anzeigen 26

R

read, Kurzform für ACL-Berechtigungen 36
Regeln für das Zuweisen von Gruppennamen 59
Rückrufe 5

S

Schalter bei AFS-Befehlen
abkürzen 83
definiert 81
weglassen 83
Schlüsselwort für Befehl apropos 87
Sicherheit in AFS 6
Stammverzeichnis des AFS-Dateibereichs 2
Standort, definiert 2
Status der Datei-Server-Maschinen 29
Syntax der beschriebenen AFS-Befehle 81
system:administrators, Gruppe 38
system:anyuser, Gruppe
in ACLs verwenden 38
system:authuser, Gruppe 38
Systemverwaltungsgruppen
in ACLs verwenden 38

T

Token
als Nachweis der Authentifizierung 6, 14
Anzeigen 17
Benutzung bei der gegenseitigen Authentifizierung 7
Lebensdauer 16
Zerstören 19
tokens
Befehl 17
getting 16

Ü

Überprüfen
Token 17

U

UID, AFS 57
UNIX, Unterschiede zu AFS
anmelden 8
Befehle 10
Dateiübertragung 8
Dateizugriff/-Zugriffsschutz 9
gemeinsame Benutzung von Dateien 8
Kennwörter 9
Modusbits, Interpretation 50
Unterverzeichnisse, Zugriff 34, 39

V

verteiltes Dateisystem 1
Verweigern des Zugriffs mit negativem ACL-Eintrag 45
Verzeichnis afs (/afs)
als Stammverzeichnis des AFS-Dateibereichs 2, 21
Verzeichnisse
ACL ersetzen 46
ACLs von einem Verzeichnis in ein anderes kopieren 48
Fehler beim Zugriff 69
Kurzform für die Referenz 84
Standort anzeigen 28
Zugreifen auf AFS 21
Verzeichnisse *(Forts.)*
Zugriff erteilen 43
Zugriff verweigern 45
Zugriffssteuerungsliste definieren 33
Volumes
definiert 3
Interaktion zwischen Volume und Mount-Punkt 4
Zugreifen über Mount-Punkte 3

W

write, Kurzform für ACL-Berechtigungen 36

Y

you don't have the required access rights (Fehlernachricht) 73

Z

Zellen
definiert 2
lokal vs. fremd 3
Zugriff auf AFS-Dateibereich
auf Verzeichnisebene steuern 34
Fehler, Fehlerbehebung 69
Format von Pfadnamen 21
für Benutzer erteilen und verweigern 33
für Benutzer fremder Zellen aktivieren 40
für Serviceprozesse aktivieren 39
Steuerung von ACL-Einträgen 43
Steuerung von Unterverzeichnissen 39
von NFS-Client-Maschine 75
Zugriffsberechtigungen in ACL
siehe Einträge: *Berechtigungen in ACL, ACL* 34
Zugriffscodemarkierung a zu Gruppen 65
Zugriffscodemarkierung m zu Gruppen 65
Zugriffscodemarkierung o zu Gruppen 65
Zugriffscodemarkierung r zu Gruppen 65
Zugriffscodemarkierung s zu Gruppen 65
Zugriffscodemarkierungen zu Gruppen 65
Zugriffsschutz
für Dateien und Verzeichnisse 33

Zugriffsschutz *(Forts.)*
Gruppeninformationen 65
Zugriffsschutzdatenbank 85
Zugriffssteuerungsliste
siehe Eintrag: *ACL* 33
Zusätzliche ACL-Berechtigungen 36

Bemerkungen

Erste Ausgabe (April 2000)

Diese Informationen wurden für in den USA angebotene Produkte und Services erstellt.

IBM darf die in diesem Dokument beschriebenen Produkte, Services oder Funktionen in anderen Ländern nicht anbieten. Informationen über die gegenwärtig im jeweiligen Land verfügbaren Produkte und Services sind beim IBM Ansprechpartner erhältlich. Hinweise auf IBM Lizenzprogramme oder andere IBM Produkte bedeuten nicht, daß nur Programme, Produkte oder Serviceleistungen von IBM verwendet werden können. Anstelle der Produkte, Programme oder Serviceleistungen können auch andere ihnen äquivalente Produkte, Programme oder Serviceleistungen verwendet werden, solange diese keine gewerblichen oder andere Schutzrechte verletzen. Es liegt jedoch in der Verantwortung des Benutzers, den Einsatz nicht von IBM stammender Produkte, Programme oder Services zu bewerten und überprüfen.

Für die in diesem Artikel beschriebenen Produkte und Verfahren kann es IBM Patente oder Patentanmeldungen geben. Mit der Auslieferung dieser Veröffentlichung ist keine Lizenzierung dieser Patente verbunden. Lizenzanforderungen sind schriftlich und in englischer Sprache zu richten an:

IBM Europe
Director of Licensing
92066 Paris
La Defense Cedex
U.S.A.

Lizenzanfragen zu DBCS-Informationen (Double-Byte Character Set) sind an die IBM Abteilung für geistige Eigentumsrechte Ihres Landes zu richten, oder senden Sie schriftliche Anfragen an:

IBM World Trade Asia Corporation Licensing
2-31 Roppongi 3-chome, Minato-ku
Tokyo 106, Japan

Der folgende Absatz gilt nicht für Großbritannien und jedes Land, in dem Bestimmungen dieser Art mit den dortigen Rechtsvorschriften nicht vereinbar sind:

“”

© Copyright IBM Corp. 1989, 2000

Trotz sorgfältiger Bearbeitung können technische Ungenauigkeiten oder Druckfehler in dieser Veröffentlichung nicht ausgeschlossen werden. Änderung des Textes bleibt vorbehalten.

Verweise in diesen Informationen auf WWW-Sites anderer Anbieter dienen lediglich als Benutzerinformationen und stellen keinerlei Billigung des Inhalts dieser WWW-Sites dar. Das über diese WWW-Sites verfügbare Material ist nicht Bestandteil des Materials für dieses IBM Produkt. Die Verwendung dieser WWW-Sites geschieht auf eigene Verantwortung.

Werden an IBM Informationen eingesandt, können diese beliebig verwendet werden, ohne daß eine Verpflichtung gegenüber dem Einsender entsteht.

Lizenznehmer des Programms, die Informationen zu diesem Produkt wünschen mit der Zielsetzung: (i) den Austausch von Informationen zwischen unabhängigen, erstellten Programmen und anderen Programmen (einschließlich des vorliegenden Programms) sowie (ii) die gemeinsame Nutzung der ausgetauschten Informationen zu ermöglichen, wenden sich an folgende Adresse:

Director of Licensing
ATTN: Software Licensing
11 Stanwix Street
Pittsburgh, PA 15222-1312
U.S.A.

Die Bereitstellung dieser Informationen kann unter Umständen von bestimmten Bedingungen - in einigen Fällen auch von der Zahlung einer Gebühr - abhängig sein.

Die Lieferung des im Handbuch aufgeführten Lizenzprogramms sowie des zugehörigen Lizenzmaterials erfolgt im Rahmen der Allgemeinen Geschäftsbedingungen der IBM oder einer äquivalenten Vereinbarung.

Alle in diesem Dokument enthaltenen Leistungsdaten stammen aus einer gesteuerten Umgebung. Die Ergebnisse, die in anderen Betriebsumgebungen erzielt werden, können daher erheblich von den hier erzielten Ergebnissen abweichen. Einige Daten stammen möglicherweise von Systemen, deren Entwicklung noch nicht endgültig ist. Eine Garantie, daß diese Daten auch in allgemein verfügbaren Systemen erzielt werden, kann nicht gegeben werden. Darüber hinaus wurden einige Daten unter Umständen durch Extrapolation berechnet. Die tatsächlichen Ergebnisse können abweichen. Benutzer dieses Dokuments sollten die entsprechenden Daten in ihrer spezifischen Umgebung prüfen. Diese Daten stellen deshalb keine Leistungsgarantie dar.

Informationen über Produkte anderer Hersteller als IBM wurden von den Herstellern dieser Produkte zur Verfügung gestellt, bzw. aus von ihnen veröf-

fentlichten Ankündigungen oder anderen öffentlich zugänglichen Quellen entnommen. IBM hat diese Produkte nicht getestet und übernimmt im Hinblick auf Produkte anderer Hersteller keine Verantwortung für einwandfreie Funktion, Kompatibilität oder andere Ansprüche. Fragen hinsichtlich des Leistungsspektrums von Produkten anderer Hersteller als IBM sind an den jeweiligen Hersteller des Produkts zu richten.

Alle Aussagen zur zukünftigen Richtung oder Absicht von IBM können ohne vorherige Ankündigung geändert oder zurückgenommen werden. Hierbei handelt es sich nur um Ziele und Zielsetzungen. Die oben genannten Erklärungen bezüglich der Produktstrategien und Absichtserklärungen von IBM stellen die gegenwärtige Absicht der IBM dar, unterliegen Änderungen oder können zurückgenommen werden, und repräsentieren nur die Ziele der IBM.

Alle ausgewiesenen IBM Preise sind von IBM empfohlene aktuelle Einzelhandelspreise und können ohne besondere Hinweise geändert werden. Die Verkaufspreise der Händler können davon abweichen.

Diese Informationen dienen ausschließlich Planungszwecken. Die hierin enthaltenen Informationen stehen unter dem Vorbehalt ihrer Änderung, bevor die beschriebenen Produkte öffentlich zugänglich werden.

Diese Veröffentlichung enthält Beispiele für Informationen des alltäglichen Geschäftsablaufes. Sie sollen nur die Funktionen des Lizenzprogrammes illustrieren; sie können Namen von Personen, Firmen, Marken oder Produkten enthalten. Alle diese Namen sind frei erfunden, Ähnlichkeiten mit tatsächlichen Namen und Adressen sind rein zufällig.

Wenn Sie diese Veröffentlichung als Softcopy betrachten, werden Fotografien und Farbabbildungen möglicherweise nicht angezeigt.

Marken

Die folgenden Begriffe sind Marken der International Business Machine Corporation in den Vereinigten Staaten oder anderen Ländern:

AFS
AIX
AS/400
CICS
CICS OS/2
CICS/400
CICS/6000
CICS/ESA
CICS/MVS
CICS/VSE
CICSPlex
DB2
DCE Encina Lightweight Client
DFS
Encina
IBM
IMS
MQSeries
MVS/ESA
OS/2
OS/390
OS/400
PowerPC
RISC System/6000
RS/6000
S/390
Transarc
TXSeries
VSE/ESA
VTAM
VisualAge
WebSphere

Microsoft, Windows, Windows NT und das Windows-Logo sind Marken der Microsoft Corporation in den Vereinigten Staaten oder anderen Ländern.

Sun, SunLink, Solaris, SunOS, Java, alle auf Java basierenden Marken und Logos, NFS und Sun Microsystems sind Marken oder eingetragene Marken der Sun Microsystems, Inc. in den Vereinigten Staaten oder anderen Ländern.

UNIX ist eine eingetragene Marke in den Vereinigten Staaten oder anderen Ländern und wird ausschließlich über X/Open Company Limited lizenziert.

Andere Namen von Unternehmen, Produkten oder Serviceleistungen können Marken anderer Unternehmen sein.

Antwort

AFS
Benutzerhandbuch

IBM Form GC12-2831-00

Anregungen zur Verbesserung und Ergänzung dieser Veröffentlichung nehmen wir gerne entgegen. Bitte informieren Sie uns über Fehler, ungenaue Darstellungen oder andere Mängel.

Zur Klärung technischer Fragen sowie zu Liefermöglichkeiten und Preisen wenden Sie sich bitte entweder an Ihre IBM Geschäftsstelle, Ihren IBM Geschäftspartner oder Ihren Händler.

Unsere Telefonauskunft ″HALLO IBM″ (Telefonnr.: 01803/31 32 33) steht Ihnen ebenfalls zur Klärung allgemeiner Fragen zur Verfügung.

Kommentare:

Danke für Ihre Bemühungen.

Sie können ihre Kommentare betr. dieser Veröffentlichung wie folgt senden:

- Als Brief an die Postanschrift auf der Rückseite dieses Formulars
- Als FAX an die folgende Nummer: 01-412-667-4380 (USA und Kanada; Auslandsgebühren werden fällig)
- Als E-Mail an die folgende Adresse: fsdoc@us.ibm.com

Name	Adresse
Firma oder Organisation	
Rufnummer	E-Mail-Adresse

Antwort
GC12-2831-00

IBM Corporation
ATTN: File Systems Documentation Group
11 Stanwix Street
Pittsburgh, PA

Programmnummer:

Gedruckt in Deutschland

GC12-2831-00

Spine information:

AFS Benutzerhandbuch Version 3.6 GC12-2831-00